

## AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY POLICY

1. **SCOPE/EFFECT:** This Medical Center Policy (MCP) affects all Medical Center employees, research personnel, students, Home Base Primary Care Program, contractors, and/or volunteers who are involved in the management, use or operation of each federal computer system within or under the supervision of that agency. There have been major changes throughout this policy.

### 2. **PURPOSE:**

a. This policy establishes policy, responsibilities, and procedures for the security of *Network 4*, information systems. The security program is designed to protect all Information Technology (IT) Systems and telecommunications resources from unauthorized access, disclosure, modification, destruction, or misuse. These provisions comply with the Office of Cyber and Information Security (OCS) policy and guidelines, Federal IT security laws and regulations, including VA Handbook 6500, the Computer Security Act of 1987(PL 100-235), Office of Management and Budget (OMB) Circular A-130 and its appendices, Federal Information Security Management Act of 2002 (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and National Institute of Standards and Technology (NIST) guidance. This policy applies to all Medical Center staff as well as Community Based Outpatient Clinics (CBOCs), Home Based Primary Care Program (HBPCs) staff, and the security of all information that is collected, transmitted, used, processed, stored, or disposed of, by or under the direction of this operating unit or its contractors.

b. For the purpose of this document, the term “sensitive data” refers to information whose loss, misuse, or unauthorized access to (or modification of) could adversely affect the national or departmental interest or the conduct of Federal or departmental programs or the privacy to which individuals are entitled. This information includes but is not limited to the business administrative, medical, benefits, personal and individually identified health information in electronic and copyright-protected software or any other form.

c. In this document, the term workforce refers to on-site or remotely located employees, contractors, students, Without Compensation (WOC), volunteers, and any other appointed workforce members.

d. In this document, the term workstation refers to personal computers, thin clients, and laptops/notebooks.

### 3. **POLICY:**

a. The Information Security Officer (ISO) will develop, implement, maintain, and enforce a structured program to safeguard all information technology assets. The security program is designed to ensure the continued operation of mission-critical activities and the integrity, availability, confidentiality, and authenticity of data and information; protect our assets from

theft, misuse, and unauthorized use; and develop a continuing awareness of the need for, and the importance of, IT security within facility, HBPCs and CBOCs.

b. All users of facility's systems are responsible for complying with this security policy, as well as procedures and practices developed in support of this policy. All users responsible for implementing the policy and procedures will have this document made available. Violations of security policy or procedures will be brought to the attention of the appropriate management for appropriate disciplinary action and reported in accordance with national and local IT Incident Reporting policy.

c. All policies, procedures, and any actions/activities taken as a result of these policies must be documented and retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

d. All documentation related to the information security program will be reviewed annually and updated as needed in response to environmental or operational changes affecting the security of the sensitive data.

e. Sites can append site-specific clarifications or site-specific procedures to the procedure section of a control as long it does not alter the content of the original procedure or lessen the authority of the control. Sites cannot alter the Policy section of the control.

f. Detailed policies and procedures required by applicable laws are found in the attachments.

#### 4. PROCEDURE:

See attachments:

Attachment A – Management Control Procedures

Attachment B – Operational Control Procedures

Attachment C - Technical Control Procedures

Attachment D - Acronyms

#### 5. RESPONSIBILITY:

a. Executive Management, through the Information Security Officer (ISO), is responsible for:

(1) Providing the necessary resources (funding and personnel) to support the Information Security Program and ensuring that the Facility meets all the information security requirements mandated by Executive and VA policy and other federal legislation (e.g., FISMA, HIPAA).

(2) Safeguarding IT assets via funds and personnel allocation, and ensuring that the Facility meets all the information security requirements mandated by Executive and VA policy and other federal legislation (e.g., FISMA, HIPAA).

(3) Ensuring there is adequate ISO coverage for the facilities and associated clinics. The Facility ISO will report directly to OI&T'S Network ISO (NISO) with substantive oversight provided by the Medical Center Director or Associate Director.

(4) Ensuring the Facility ISO is fully involved in all new projects concerning the development or acquisition of systems, equipment, or services including risk analysis, security plans, requests for proposal (RFPs), and other procurement documents that require the ISO's participation.

(5) Ensuring the Facility ISO is made a part of the clearance from indebtedness procedure in a manner that effectively assures access is terminated. This will allow the ISO to ensure all users are deactivation from the facility system as well as any remote systems.

(6) Ensuring that all computer security incidents are reported to the Facility ISO that will report to the VA-NSOC within one hour of notification of the incident in accordance with, current National Guidelines. The Facility ISO will notify the local Incident Resolution Team (IRT) and the Network 4 ISO.

(7) Ensuring that system users attend formal information security training. This training must include but not be limited to: information security orientation for new hires; information security training when new duties are assigned or when new access is granted and new security responsibilities will result; and annual security awareness security training for current employees. Attendance at information security training shall be documented, and reported to the Facility ISO as requested.

(8) Ensuring that the Facility ISO, Information Manager/CIO, Privacy Act Officer, Chief of Human Resources, Contracting Officers, local managers, and sensitive system users complies with all their responsibilities listed below.

b. Facility Information Security Officer (ISO): Implementation of an effective security program in accordance with Office of Cyber and Information Security policy, applicable federal laws and regulations, and guidelines at the facility. Activities include, but are not limited to:

(1) Coordinating, establishing, facilitating, and updating any additional information security policies and procedures.

(2) Establishing effective working relationships with facility Privacy Officer, Freedom of Information Act (FOIA) Officer, Privacy Act Officer, Contracting Officer, and Human Resources personnel to assure IT security and HIPAA/FOIA/PA/FISMA policies complement and support each other.

(3) Monitoring the facility Information Security Program to ensure that appropriate and timely action is taken to protect assets from damage, destruction, alteration and misappropriation.

(4) Recommending appropriate alternate ISO coverage to the facility Director and their NISO.

(5) Maintaining documentation of incidents related to information security and their resolutions. Reporting these incidents to VA-Security Operations Center (SOC) and management as appropriate.

(6) Ensuring mechanisms are established to document requests for access to sensitive automated information systems, to ensure that access requests are reviewed and approved, and to report and resolve violations of information security by contractors and VA employees

(7) Ensuring user awareness of information security by providing employee orientation, training, and continued awareness to the workforce. Ensuring that risk analyses and contingency plan testing is performed and approved recommendations or corrective actions are implemented.

(8) Reporting violations of IT security policies, procedures, and accepted practices to VA-NSOC, the NISO or an OCS official, as appropriate.

(9) Reviewing and evaluating the impact of proposed facility changes to the information security program.

(10) Performing information security program assessments.

(11) Ensuring all appropriate IT business continuity plans and disaster recovery plans are developed, tested, and maintained.

(12) Ensuring procedures are established for identifying actual or suspected computer security incidents and for investigating, mitigating, and reporting such incidents.

(13) Monitoring systems and user activity regularly and maintain logs of reviews.

(14) Participating in local and Network 4 IT security meetings and initiatives.

(15) Auditing the media sanitization process in accordance with VA guidelines.

(16) Participating in Federal Information Security Management Act (FISMA) activities to include, but not limited to, timely updating of SMART database; coordinate remediation of identified deficiencies with local and Network 4 staff.

(17) Ensuring Certification and Accreditation (C&A) of information systems.

(18) Ensuring that HIPAA security requirements are implemented at the facility.

(19) Completing the vulnerability scans for all IT systems within the area of responsibility.

(20) Ensuring the remediation actions are taken from the results of vulnerability scans and/or VA-NSOC alerts.

(21) Serve as a member of the Institutional Review Board (IRB), Environment of Care, Periodic Performance Review, and Research Development (R&D) committees

(22) Ensuring all equipment potentially containing sensitive data has been sanitized in accordance with OCS mandates before final disposition.

c. Facility Chief Information Officer (FCIO) or designee is responsible for:

(1) Working closely with ISO to provide technical advice and other assistance dealing with implementation of IT security policy.

(2) Identifying each locally maintained computer system that contains sensitive information, and providing technical input into various mandated documents/reports (i.e., FISMA, C&A, HIPAA).

(3) Identifying all assets and implementing security measures, which meet established security standards and policies, in order to protect said assets on all systems under their management control.

(4) Assuring all IT staff receives security training appropriate to their job functions.

(5) Assuring all high security areas meet acceptable levels of physical security. High security areas include, but not limited to, computer room(s), telephone switch (PBX) room(s), and main telecommunications demarcation point if not located in the PBX or computer room, data/telecommunications closets, IT work areas and IT storage areas.

(6) Enforcing policy and procedure that restricts access of personnel to all computer room environments.

(7) Assuring, in coordination with ISO and supervisors, the termination of IT access of employees who no longer have a need.

(8) Authorizes and monitors the use of guest and/or anonymous and/or accounts deemed to be 'generic' (not tied to a specific user) used on any IT system with their area of responsibility.

(9) Ensures all user accounts are reviewed on a regular basis and any unneeded accounts are terminated and/or removed.

(10) Ensuring critical system files are backed up on a regular basis and are housed in a secure location far enough away from the system to not be affected by the same catastrophic event.

(11) Implementing media control policy and procedure.

(12) Assuring software security controls are implemented.

(13) Enforcing established policy for the use of non-VA hardware and software.

(14) Maintaining inventory of computer resources under their control.

(15) Implement configuration management and change controls.

d. Privacy Officer/Freedom of Information Act (FOIA) Officer

(1) Coordinating with the ISO for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule or other federal privacy statutes.

(2) Working with the facility ISO and/or NISO to assure IT security and HIPAA/FOIA/PIA/FISMA policies complement and support each other.

(3) Coordinates with the ISO and or NISO in reporting all privacy and security incidents.

e. Chief, Human Resources Management Service, and/or designees

(1) Submitting requests for obtaining background investigations on all appropriate workforce.

(2) Providing guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information security practices, laws, regulations, policies, and rules of behavior.

(3) Providing advice to supervisors and managers regarding appropriate information security related performance standards and position descriptions for employees who are authorized to access any IT system(s).

f. VA Contracting Officer/COTR (contracting officer technical representative) is responsible for:

(1) Including a specific set of IT security responsibilities in all contracts.

(2) Abide by, those responsibilities as stated in contracts with VA.

(3) Assuring background investigations of contractors in accordance with VA policy are conducted. Contracts should stipulate that the contractor is responsible for the cost of background investigations.

(4) Ensuring that business associate agreements are enacted for all contracts in which the contractor meets the definition of a business associate.

(5) Security requirements and specifications for hardware and software maintenance personnel contracted from commercial sources shall be defined and approved prior to the signing of contractual agreements.

(6) Procurement officials shall ensure negotiated contracts pertaining to IT services include a separate section dealing with information security issues specifying the level of trust required and contractor responsibility in complying with established VA requirements.

(7) Procurement officials shall ensure that all Request for Proposals (RFPs) and purchase agreements pertaining to IT hardware and software, equipment capable of storing sensitive data, or intended for connection to the computer network are reviewed for security implications as outlined in VA Handbook 6500. Such officials are responsible for the inclusion of a separate section in the contract dealing with information security issues, where appropriate.

(8) The Contracting Officer's Technical Representative (COTR) for the contract must measure contract performance and terminate the contract if security requirements are not being met.

g. Local Managers, Supervisors, and their designees (e.g. ADPAC) are responsible for:

(1) Identifying and protecting all assets within their assigned areas of management control.

(2) Protecting sensitive information generated or used by their staff from disclosure to, and/or modification by, unauthorized individuals.

(3) Ensuring sensitive information, whether computerized or printed, is secured when the work area is unattended.

(4) Noting variances from established IT security policies or procedural practices, initiating corrective actions, and notifying the ISO of all reportable incidents.

(5) Participating with the ISO and Human Resources Management Officer to determine the appropriate sensitivity level designation for positions under their control.

(6) Briefing new personnel on rules for protecting sensitive data.

(7) Ensuring that supervised personnel have only the minimum necessary access to the sensitive information required to carry out their authorized functions or assigned duties.

(8) Ensuring that access privileges of terminating and transferring staff are rescinded and periodically (no less than quarterly) reviewing the access privileges and menu options of each staff member.

(9) Ensuring each supervisee completes formal IT security training and that it is documented.

(10) Ensuring each employee signs the National Rules of Behavior.

(11) Ensuring that service/clinical center/service lines have written business continuity plans to assure continuation of operations when a computer system(s) is down.

(12) If applicable, assuring the position description of appointed ADPACs contains addendum outlining information security responsibilities of the ADPAC.

(13) Ensuring that media with sensitive data is disposed of via approved means. Data that is not destroyed at the site of production, such as areas where shredding is contracted, must be secured in locked containers or in locked areas until its removal for destruction.

h. All individuals who have access to sensitive information or locations are responsible for:

(1) Signing the National Rules of Behavior prior to gaining access to a VA Systems.

(2) Accessing the minimum necessary data for which they have authorized privileges.

(3) Maintaining confidentiality of sensitive data or information.

(4) Protecting their assigned user IDs, passwords, electronic signatures, and other access keys from disclosure.

(5) Appropriately securing sensitive printed information.

(6) Practicing good housekeeping with equipment and work areas.

(7) Logging off systems before leaving a terminal or computer unattended.

(8) Refraining from illegal reproduction or unlawful use of licensed computer software.

(9) Reporting violations of IT security to their supervisor and/or ISO.

(10) Attending IT security orientation training and completing annual refresher training as deemed necessary by service chief and/or supervisor or as required by policy.



(11) Using only government furnished equipment (GFE) and VA approved remote access software to remotely logon and access any VA computer system and information. Non-VA owned equipment may be used in certain circumstances, with an approved waiver. All of the security controls required for GFE must be utilized in approved non-VA owned equipment and must be funded by the owner of the equipment.

(12) Ensuring any GFE, information and/or software is adequately secured as defined in VA Handbook 6500.

(13) Obtaining supervisors and/or management authorization before taking any GFE, information and/or software off-site as outlined in VA Handbook 6500.

6. CUSTOMER SATISFACTION: Patient/family satisfaction issues were considered in the development of this policy.

7. REFERENCES: Computer Security Act of 1987, PL 100-235.

Privacy Act of 1974, 5 U.S.C. 552a.

Fraud and Related Activity in Connection with Access

Devices and Computers, 18 U.S.C. 1029-1030.

Electronic Communications Privacy Act of 1986, PL 99-508

Executive Order 10450, as amended.

5 CFR Part 930, Training Requirement for the Computer Security Act.

5 C.F.R. 731.101, et seq., (relating to suitability).

5 C.F.R. 732.101, et seq., (relating to National security)

5 C.F.R. 736.101, et seq., (relating to personnel investigations).

38 U.S.C. 3301, Confidential Nature of Claims.

38 U.S.C. 5705, Confidentiality of Medical Quality Assurance Records

38 U.S.C. 4132, Confidentiality of Certain Medical Records

OMB Circular A-130, Management of Federal Information Resources

OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

OMB Circular A-123, Internal Control Systems

VA Directive 0710 "Security."

VA Handbook 0710 "Security."

Circular 10-88-78, DM&S ADP Security Policy and Guidelines

FIPS PUB 31, Guidelines for Automated Data Processing Physical Security and Risk Management

FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974

FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis

FIPS PUB 83, Guidelines on User Authentication Techniques for  
Computer Network Access Control  
FIPS PUB 87, Guidelines for ADP Contingency Planning.  
NIST Special Publication 500-120, Security of Personal Computer  
Systems: A Management Guide  
NIST Special Publication 500-172, Computer Security Training  
Guidelines  
VA Handbook 6500, Information Security Program  
VA Directive 6504, Restrictions on Transmission, Transportation  
and Use of , and Access to, VA Data Outside VA Facilities,  
June 7, 2006.  
VA Stars and Stripes Healthcare Network Security Policy  
Memorandum No. 10N4-39., March 2005.  
VA Directive 6601, Removable Storage Media, February 27, 2007.  
FIPS PUB 199, Standards for Security Categorization of Federal  
Information and Information Systems

8. RESCISSION: Medical Center Policy 00S-08-788, dated April 25, 2008, same subject.

9. FOLLOW-UP RESPONSIBILITY: The Facility ISO is responsible for the contents of this Directive and the annual review of this Directive. This Directive will be reissued on or before January 2010.

10. DISTRIBUTION: Electronic Access to All Employees

11. ATTACHMENTS: A, B, C, D, E

## TABLE OF CONTENTS

<b>ATTACHMENT A - MANAGEMENT CONTROL PROCEDURES.....</b>	<b>11</b>
1.0 RISK MANAGEMENT (HIPAA 16 .308A1i; FISMA 1.0, 3.1.7, 12.2; NIST 800-53 RA).....	12
2.0 SYSTEM DEVELOPMENT LIFE CYCLE (FISMA 3.0, NIST 800-53 SA).....	13
3.0 SYSTEM ANALYSIS/IDENTIFICATION (OMB A-130) .....	14
4.0 FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) (EGOV 2002).....	15
5.0 SYSTEM SECURITY CATEGORIZATION (FIPS 199).....	15
6.0 SYSTEM INTERCONNECTIONS (HIPAA 164.308A8B1; FISMA 3.2.9, 12.2.3, NIST 800-53 CA-3).....	16
7.0 SYSTEM SECURITY PLAN (HIPAA 164.312C, 164 .308A5iiD; FISMA 5.0; 3.2.8, 3.2.10, 12.2.1, NIST 800-53 PL-2).....	16
8.0 RULES OF BEHAVIOR (HIPAA 164.308A3i; FISMA 4.1.3, 13.1.1; NIST 800-53 PL-4).....	17
9.0 SANCTIONS (HIPAA 164.3081iic; FISMA 6.1.5, NIST 800-53 PS-8).....	17
10.0 CERTIFICATION AND ACCREDITATION (HIPAA 162.308A8; FISMA 4. 0, 3.2, 12.2.5; NIST 800-53 CA-1).....	18
11.0 SYSTEM AND SERVICES ACQUISITION (FISMA 3.1.2; NIST 800-53, SA-2,4,9).....	19
12.0 CONTRACTS/BUSINESS ASSOCIATE AGREEMENTS (HIPAA 164.314A1).....	20
<b>ATTACHMENT B - OPERATIONAL CONTROL PROCEDURES.....</b>	<b>21</b>
1.0 PERSONNEL SECURITY (HIPAA 164.308A3; FISMA 6.0; NIST 800-53 PS).....	21
2.0 SEPARATION OF DUTIES (HIPAA 164.308A3ii, 164.308A3iia, 164.308A4iiB; FISMA 6.1.1, NIST 800-53 AC-5).....	24
3.0 PHYSICAL SECURITY CONTROLS (HIPAA 164.310A2ii; FISMA 7.1, 7.2.1, 8.2, 10.1, NIST 800-53 PE).....	24
4.0 IT SYSTEM HARDWARE AND ELECTRONIC MEDIA SANITIZATION AND DISPOSAL (HIPAA 164 .310D1; FISMA 8.2.0, 3.2.11 – 3.2.13, NIST 800-53 MP-6, 7).....	33
5.0 MOBILE/PORTABLE/WIRELESS SYSTEMS (FISMA 7.3, NIST 800-53 AC-19).....	35
<i>Blackberry wireless remote service can be used within VISN 4 if the following conditions are met:</i> .....	38
6.0 CONTINGENCY PLANNING (HIPAA 164 .308A7i; FISMA 9.0, 12.1.8, NIST 800-53 CP).....	39
7.0 IT SYSTEM HARDWARE AND SOFTWARE MAINTENANCE (FISMA 3.1. 4, 10.0, NIST 800-53 CM).....	43
8.0 DATA INTEGRITY (HIPAA 164 .312C1, 164 .312C2; FISMA 11.0, NIST 800-53 SI).....	47
9.0 SECURITY DOCUMENTATION (HIPAA 164 .306; FISMA 12.0, NIST 800-53 SA).....	48
10.0 SECURITY TRAINING, EDUCATION, AND AWARENESS (HIPAA 164.308A5; FISMA 13.0, NIST 800-53 AT).....	49
11.0 INCIDENT RESPONSE CAPABILITY (HIPAA 164.308A6ii; FISMA 14.0, NIST 800-53 IR).....	50
<i>REPORTABLE INCIDENTS – VA-NSOC</i> .....	55
<b>ATTACHMENT C - TECHNICAL CONTROL PROCEDURES.....</b>	<b>56</b>
1.0 IDENTIFICATION AND AUTHENTICATION (HIPAA 164.312A1, 164.312A2, 164.312D; FISMA 15.1.1, 15.2.2, NIST 800-53 IR).....	56
2.0 LOGICAL ACCESS CONTROLS (HIPAA 164.308A4iiB, 164.308A4iiC; FISMA 15.1, 16.1, 6.2.4, NIST 800-53 AC).....	64
3.0 LOG-ON WARNING BANNERS (HIPAA 164.310B).....	79
4.0 PENETRATION TESTING AND VULNERABILITY SCANNING (HIPAA 164.308A1i).....	79
5.0 AUDITS AND REVIEWS (HIPAA 164.312B; FISMA 17.1.1, NIST SP 800-53 AC-2, AC-13, AU-3, AU-4, AU-5, AU-6, AU-11).....	80
<b>ATTACHMENT D - ACRONYMS.....</b>	<b>84</b>

## **Management Control Procedures**

### **1.0 Risk Management (HIPAA 16 .308a1i; FISMA 1.0, 3.1.7, 12.2; NIST 800-53 RA)**

#### **Policy:**

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with all federal security statutes.

#### **Procedure:**

a. Risk Assessments: The ISO, in collaboration with the IT Managers, is responsible for conducting accurate and thorough risk assessments to estimate potential risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the facility in accordance with NIST SP 800-30, Risk Management Guide for Information Technology Systems. The assessments will review threats to the facility's IT systems, data, users, assess the probability of occurrence for potential losses and their effect, and recommend cost effective measures to reduce the facility's exposure to potential threats such as physical destruction or theft of physical assets; loss or destruction of data and program files; theft of information; theft of indirect assets; and delay or prevention of computer processing. A mission/business impact analysis will be conducted along with the risk assessments.

Every risk assessment is made up of three components, facility risk assessment, identification of systems, and system risk assessment. VA designates system owners to perform risk assessments for all information systems that are owned and operated by the facility, business partners or contractors, regardless of their location.

Risk assessment methodology encompasses nine primary steps. They are:

1. Determine system characterization by reviewing: hardware; software; system interfaces; data and information; and people.
2. System mission.
3. Identify any vulnerability or weaknesses in security procedures or safeguards.
4. Identify events that can negatively impact security (natural and manmade).
5. Identify current controls in place.
6. Identify the potential impact that a security breach could have on an organization's operations or assets, including loss of integrity, availability, or confidentiality.
7. Recommend security controls for the information and the system, including all the technical and non-technical protections in place to address security concerns.
8. Determine residual risk.
9. Document all outputs and outcomes from the risk assessment activities. This facility consolidates all lists of outputs and outcomes into a single list of documented risks (best practice).

The Facility will maintain current information/list on known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources. To ensure standardization and completeness of assessments, the facility will use the Office of Cyber and Information Security's approved risk assessment tool. The ISO, IT managers, and system managers will form a risk management team to collaborate to answer the multi-user system and facility questionnaires. A risk factor is calculated, weaknesses are identified, and a risk level is assigned.

b. **Risk Mitigation:** The ISO will review the risk assessment reports and recommendations and work with the IT managers, system administrators, and facility staff to mitigate the risks that are currently solvable. These mitigation decisions, additional procedures (if applicable) and responsibilities assigned will be documented and maintained by the ISO. The risk management team conducts a follow-up analysis to determine whether the security requirements and changes made adequately mitigate the vulnerabilities. The outstanding risks will be presented to the Director for his/her review and action. The Director may accept the risks, provide necessary resources to mitigate the risk immediately, temporarily accept the risk and define future plans for risk mitigation, or disapprove use of the system. The decisions by the Director will be maintained on file by the ISO. If additional hardware, software, or services are needed to adequately protect information and reduce risks, the following issues should be considered:

1. Applicability of the IT solution to the intended environment
2. The sensitivity of the data
3. The facility's security policies, procedures and standards
4. Other requirements such as resources available for operation, maintenance, and training.

c. **On-going Evaluations:** Risk assessments will be completed at least every three years by the appropriate risk management team or after a significant audit finding or when the information system experiences significant enhancement or modification. Examples of significant enhancements or modifications include change in operating system, change in hardware, change in the overall operating environment, and major system upgrades.

## **2.0 System Development Life Cycle (FISMA 3.0, NIST 800-53 SA)**

### **Policy:**

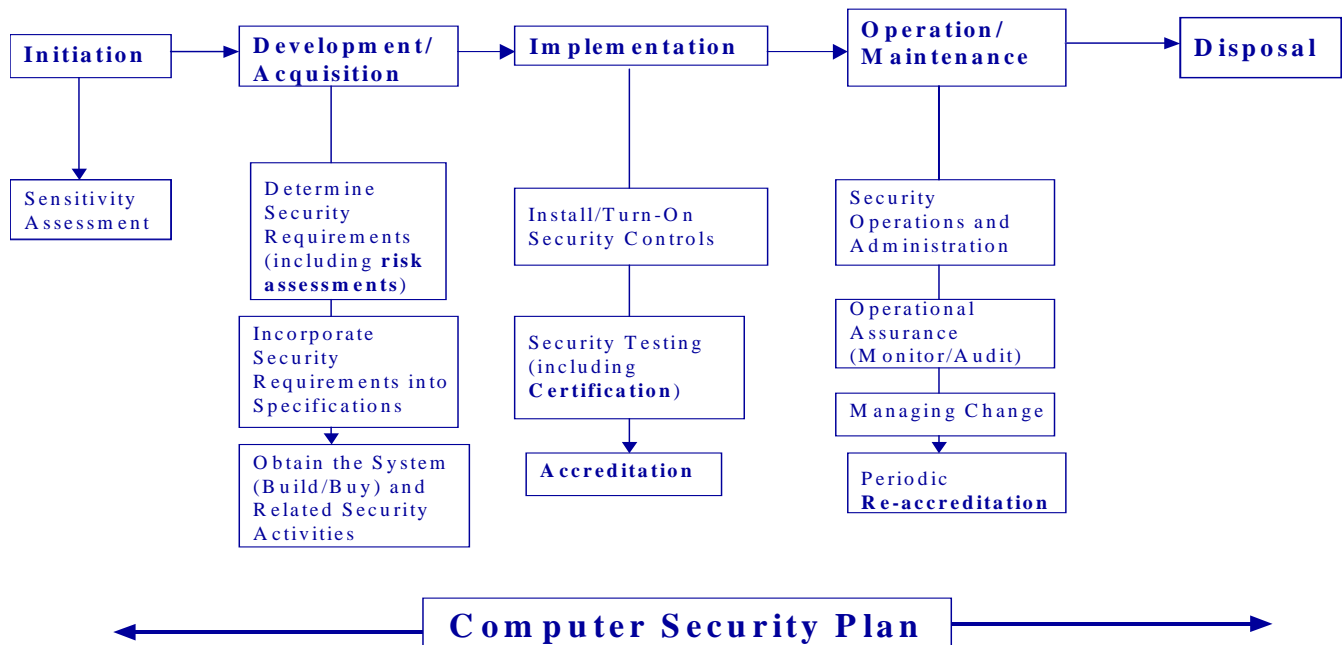
The Facility manages the information systems using a system development life cycle methodology that includes information security considerations. The Facility designs and implements their information systems using security engineering principles.

### **Procedure:**

The system development life cycle is a proven series of steps and tasks used to build and maintain quality systems faster, at lower costs, and with less risk. Each IT system in the Facility operates in one of the below stages of system development. Any locally developed system will follow the life cycle steps and be certified and accredited prior to implementation; during the development of any system within the Facility, security requirements will be defined. The information system developer creates and implements a configuration management plan that

controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation. The information system developer also creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

These are the steps of the system development lifecycle:



### 3.0 System Analysis/Identification (OMB A-130)

#### Policy:

All automated information resources that collect, process, transmit, store, or disseminate VA information must be identified, regardless of ownership.

#### Procedure:

The Facility will include all automated information resources operated by the facility personnel or by contractors in support of VA work. The system owners and system managers working with the ISO will identify and analyze the system's boundaries and organizational responsibilities by utilizing the following four NIST criteria:

- Be under the **same** direct management control. Direct management control does not necessarily imply that there is no intervening management. It is also possible for an information system to contain multiple subsystems. (For definition of subsystem see NIST SP 800- 18, Revision 1, page 9).

- 
- Have the **same** function or mission objective;
- Have essentially the **same** operating characteristics and security needs; and
- Reside in the **same** general operating environment.

## **4.0 Federal Information Security Management Act (FISMA) (egov 2002)**

### **Policy:**

The Facility will conduct, as mandated by FISMA, an annual self-assessment survey for all applicable systems within the operating unit's control. Deficiencies identified during this assessment will be mitigated and documented on an on-going basis.

### **Procedure:**

The Federal Information Security Management Act (FISMA) survey provides a local review of the security controls of the system, the system boundary, and its interconnected systems. To meet this requirement, systems must be entered into the VA FISMA/Security Management and Report Tool (SMART) database. Systems can be combined into groups based on system identification. Systems can be added or deleted from the FISMA/SMART database periodically based on their system life cycle designation. ISOs, system owners, system managers, and IT management will complete the questionnaire. It documents the security controls in place, the plans of actions and milestones (POA&M) to remediate any deficiencies noted, the anticipated completion date, and the actual completion date.

## **5.0 System Security Categorization (FIPS 199)**

### **Policy:**

All VA information systems must have their security categorized in accordance with Federal Information Processing Standards (FIPS) 199 and must document the results of this categorization in the system security plan. Designated VA OCS staff review and approve the security categorizations as part of the Certification and Accreditation (C&A) process in accordance with NIST 800-37. The VA Privacy Office conducts a privacy impact assessment on information systems based on OMB Memorandum 03-22.

Security categorization standards for information systems provide a common framework and understanding for expressing security that, for the Federal government, promotes: (i) effective management and oversight of information security programs.

### **Procedure:**

The determination of an information systems security categorization will be made in accordance with FIPS 199 so that the appropriate controls can be implemented throughout the system development life cycle (SDLC). The ISO, utilizing OCS and NIST 800-60 (Guide for Mapping

Types of Information and Information Systems to Security Categories) guidance, will work with the system managers/IT management in determining the sensitivity for each system within their facility.

## **6.0 System Interconnections (HIPAA 164.308a8b1; FISMA 3.2.9, 12.2.3, NIST 800-53 CA-3)**

### **Policy:**

The Network 4 ISO authorizes connections (physical and wireless) from the local information systems to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. IT and the ISO approve information system interconnection agreements. A System Interconnection Agreement (SIA) is not needed with internal agency systems if an agency manages and enforces a rigid system development life cycle, which requires approvals and sign-offs ensuring compliance with security requirements.

### **Procedure:**

The Network 4 facilities must prepare a Memorandum of Understanding (MOU), stating the terms and conditions for sharing data and information resources, and a System Interconnection Agreement (SIA), specifying the technical and security requirements for the connection, for each system interconnection. The MOU and SIA will be obtained prior to connection with other systems and/or sharing of sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems.

## **7.0 System Security Plan (HIPAA 164.312c, 16 4 .308a5iiD; FISMA 5.0; 3.2.8, 3.2.10, 12.2.1, NIST 800-53 PL-2)**

### **Policy:**

Every IT system's controls within the Network 4 must be included/covered by a system security plan (SSP). The plan will contain all the elements outlined in NIST Special Publication 800-18, Revision 1, "Guide for Developing Security Plans for Information Technology Systems" as well as the appropriate security controls as outlined in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems."

### **Procedure:**

The plans provide an overview of system security requirements and controls that are in place or planned for meeting those requirements. The plans are used to document information on system characterization, management controls, operational controls, and technical controls. The SSPs are living documents, developed during the design phase and updated throughout the entire lifecycle. The SSPs are a major component in completing the certification and accreditation for the system and will be reviewed and approved by the Certification Agent (CA) and the Designated Approving Authority (DAA) within OCS. The system managers and IT management,



in close coordination with the ISO, are responsible for ensuring that SSPs are developed, reviewed annually, and maintained for each system within their area of responsibility. Significant changes are identified in the configuration management process. A summary of the security plans for each facility's systems will be included in the overall facility IT strategic plan. The ISO plays an active role in reviewing SSPs as well as providing guidance on the security impact of changes to the system. Sites will utilize the templates provided by VA in developing their site and system security plans.

### ***8.0 Rules of Behavior (HIPAA 164.308a3i; FISMA 4.1.3, 13.1.1; NIST 800-53 PL-4)***

#### **Policy:**

Rules of Behavior (ROB) are required by OMB Circular A-130, Appendix III and by the security controls contained in NIST SP 800-53. All individuals who use or gain access to VA information systems or sensitive information must sign and adhere to the Rules of Behavior that bind them to the legal and moral responsibility of preventing unauthorized disclosure before they can be authorized access to VA information systems.

#### **Procedure:**

The Facility will use the National Rules of Behavior identified in VA Handbook 6500. In the event VA Handbook 6500 is not signed the site is required to establish a set of rules that describes the responsibilities and expected behavior with regard to information system usage. These rules clearly delineate security responsibilities and expected behavior of all system owners, users, operators, and administrators. The rules include the consequences of inconsistent behavior or non-compliance. The rules include all significant aspects of information system use, including policy on use of electronic mail. The entire workforce of Network 4 will have access to a copy of these rules of behavior for review. A signed (manually or electronically) acknowledgement of these rules is a condition of access to any VA IT system. Controls to be covered in rules of behavior include:

- Responsibilities, expected use of system, and behavior of all user
- Appropriate limits on interconnections
- Consequences of behavior not consistent with rules
- Work at home rules
- Connection to the Internet rules
- Use of copyrighted work rules
- Unofficial use of government equipment rules
- Assignment and limitations of system privileges and individual accountability
- Password usage
- Searching databases and divulging information

### ***9.0 Sanctions (HIPAA 164.3081iic; FISMA 6.1.5, NIST 800-53 PS-8)***

**Policy:**

The Facilities will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures, and the National Rules of Behavior. The sanctions process is included as part of Human Resource's policies and procedures for the facility.

**Procedures:**

The responsible ISO will determine and provide evidence of a security violation. The employee's supervisor will determine appropriate action and may take, in conjunction with human resources the necessary steps and apply appropriate sanctions for employees who are non-compliant with the security policies and procedures. Actions may include, but are not limited to, progressive discipline or other resolutions. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions as a result of a HIPAA security complaint.

***10.0 Certification and Accreditation (HIPAA 162.308a8; FISMA 4. 0, 3.2, 12.2.5; NIST 800-53 CA-1)***

**Policy:** VA authorizes all systems for processing before operations and updates the authorization every three years. All Network 4 systems must be certified and accredited in accordance with NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" and VA guidance. Security certification and accreditation are important activities that support a risk management process and are an integral part of this Network 4's information security program. VA officials sign and approve the security accreditation.

**Procedure:** The initiation phase consists of three tasks: (1) preparation; (2) notification and resource identification; and (3) system security plan analysis, update, and acceptance. This phase requires that the appropriate security controls based on NIST SP 800-53 are instituted and documented in the system security plan.

The Facility conducts an assessment of the security controls in their information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the systems. The security certification phase consists of three tasks: (1) security control assessment; (2) security certification documentation; and plan of action and milestones. Testing is required to certify that the system meets security requirements and must be accomplished prior to receiving full accreditation. Testing validates compliance of the fully integrated system with the security policy and requirements stated in the system's documentation. It is necessary to produce evidence that this is accomplished by conducting a system test and evaluation, a penetration test, communications security evaluation, system management analysis, site evaluation, contingency plan evaluation, and risk analysis evaluation. Testing must be accomplished by a team outside of the organization responsible for the system. Using the results of the testing, the Facility then develops and updates periodically, a plan of action and milestones for the information systems that documents the facility's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the systems.

The Facility submits the required documentation to the appropriate organizational official (determined by OCS) for authorization for processing (accreditation). The security accreditation Phase consists of two tasks: (1) security accreditation decision; and (2) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities and risks are of an acceptable level of risk to the facility. A security plan, risk analysis, and a contingency plan are required to help make the appropriate decision. Upon successful completion of this phase, the system will have (1) an authorization to operate; (2) an interim authorization to operate under specific terms and conditions; or (3) denial of authorization to operate.

The continuous monitoring phase consists of three tasks: (1) configuration management and control; (2) security control monitoring; and (3) status reporting and documentation. Systems must be re-accredited by the system owner every three years or whenever a major change has been made to the system that may affect its security. Major changes include: an increase in the sensitivity/criticality of a system, an increase in threat level, policy change, a change in operating system (base platform), a change to security relevant software, a change to hardware that could affect the security architecture, an increase in interconnection with other systems outside the accreditation boundary, or significant changes in the security requirements that apply to the system.

### ***11.0 System and Services Acquisition (FISMA 3.1.2; NIST 800-53, SA-2,4,9)***

#### **Policy:**

Various external mandates (OMB Circular A-130 and the Clinger-Cohen Act of 1996) dictate that security is incorporated into systems, as well as IT capital planning and overall budget processes. All Network 4 facilities determine, document, and allocate as part of their capital planning and investment control process the resources required to adequately protect the information systems.

Outsourced Information System Services – the Facility ensures that third-party providers of information system services employ adequate security controls in accordance with local and department policy. The Facility monitors security control compliance. In contracts/agreements for hardware, software, computer-related services, or access to VA information systems appropriate security requirements, specifications, and training must be included in statements of work and security requirements and specifications should be properly implemented before the system goes into operation and through the life cycle of the system. The security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts are based on an assessment of risk.

#### **Procedure:**

The solicitation documents for information systems and services include security requirements that describe (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The ISO shall actively support the review and approval of all acquisition requests for IT products and services

requested by their facility in accordance with their local Acquisition & Materiel Management (A&MM) Service policies and procedures. Their review is to ensure security is addressed throughout a system's life cycle, from mission and business planning through disposal. The ISO will participate on the local IT equipment committees to ensure security is addressed at the beginning of the life cycle of the system.

Third party providers are subject to the same information security policies and procedures as the facility, and must conform to the same security control and documentation requirements as would apply to the facility's internal systems. Appropriate facility management approves outsourcing of information system services to third party providers (e.g., contractors, other external organizations). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. The service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

### ***12.0 Contracts/Business Associate Agreements (HIPAA 164.314a1)***

#### **Policy:**

In contracts/agreements for hardware, software, and computer-related services, appropriate security requirements, specifications, and training must be included in statements of work and security requirements and specifications should be properly implemented before the system goes into operation and through the life cycle of the system. The facility contracting officer, the Privacy Officer, and the ISO will work together to identify entities that are Business Associates under the HIPAA Security Rule and ensure that Business Associate Agreements (BAAs) are enacted for all Business Associates in accordance with HIPAA BAA policies and procedures.

#### **Procedure:**

All contracts, agreements, and relationships must be assessed to determine if a business associate relationship exists. A business associate relationship exists if the facility is required to release protected health information to a contractor or business partner in order for them to provide services on the facility's behalf. If a business associate relationship is determined to exist, a business associate agreement must be enacted utilizing VHA HIPAA Program-approved BAA language. If a business associate is determined to serve more than one VA medical center, a national BAA may be enacted through the VHA HIPAA Program Office. BAAs must be kept updated and documentation of agreements must be maintained as long as the agreement is in force.

## **Operational Control Procedures**

### ***1.0 Personnel Security (HIPAA 164.308a3; FISMA 6.0; NIST 800-53 PS)***

#### **Policy:**

The Facility has established personnel controls in accordance with NIST 800-53, HIPAA and VA policy that include, but are not limited to, screening, position descriptions, position sensitivity designations, transfer and termination procedures, and background investigations.

#### **Procedure:**

a. **Screening (HIPAA 164.308a3iiB)**: Screening will be conducted for both federal and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to sensitive data or information. The Contracting Officer will ensure screening is conducted for all contract personnel and Human Resources personnel will ensure that screening is conducted for federal employees and all other appointed workforce members.

b. **Position Descriptions**: Supervisors will write position descriptions reflecting specific security responsibilities. Within this context, "specific security responsibilities" refer to employee obligations to protect sensitive data and to use such data, and the information derived from it, only in the execution of official duties. In conjunction with supervisors and the ISO, Human resources will annotate position descriptions with the sensitivity level designations. Human resources will use these designations to determine the appropriate background investigation level. Procedures for determining position sensitivity level shall be performed in accordance with FPM Chapters 731 and 732 and departmental guidelines, and documented on VA Form 50-2280. An assessment of all designations shall be done on a continuing basis in order to identify any changes in the data available or the duties and responsibilities of the position that would cause the position to be placed in a higher or lower category. An example of "specific security responsibilities" is as follows:

c. **ADP Security**: In the performance of official duties, the employee has regular access to printed and electronic files containing sensitive data which must be protected under the provisions of the Privacy Act of 1974 and other applicable laws, federal regulations, VA statutes and policy, and VHA policy. The employee is responsible for: (1) protecting that data from unauthorized release or from loss, alteration, or unauthorized deletion and (2) following applicable regulations and instructions regarding access to computerized files, release of access codes, etc., as set out in a "Rules of Behavior" formerly known as a computer access agreement which the employee signs.

d. **Background Investigations (HIPAA 164.308a3iiB)**: The level of screening required will vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm

that could be caused by the individual. Procedures for completing background investigations are contained in VA Directive 0710 and its Handbook, "Personnel Suitability and Security Program." Further guidance can also be found in VHA Directive 0710; Appendix A. Staff with system administrator privileges, Network 4 and facility ISOs and alternates, IRM staff (excluding clerical positions), Quality Management Coordinators, Finance Officers or equivalent, and any staff with either programmer privileges or the ability to create and add users and/or menus to establish file access for AIS resources which process sensitive data, will have a sensitivity designation of no less than "critical-sensitive" (High Risk) and must receive a background investigation in accordance with VA regulations and commensurate to the position sensitivity designation. VA Form 50-4236, Certificate of Eligibility, certifies that an employee is determined eligible to occupy a position designated as sensitive. The Office of Inspector General Security Officer issues this form after a background investigation has been conducted. VA Form 50-4236 shall be maintained in an employee's Official Personnel File. When an employee in a sensitive position transfers to a non-sensitive position or is separated from VA employment, the Office of Inspector General (OIG) Security Officer shall be notified in writing so that the Certificate of Eligibility granted to that individual can be revoked. The Certificate of Eligibility remains in effect per VA Directive 0710. Human Resources shall review positions designated as sensitive on an annual basis and keep a record of the status of background investigations for review by the ISO and outside auditing bodies.

**e. Contractors (HIPAA 164.314a1):** All non-VA users having access to VA information resources through a negotiated contract, agreement, or arrangement shall meet the security levels defined by the contract, agreement, or arrangement. Such users will read and sign the National Rules of Behavior and take security awareness training prior to receiving access to the information systems. Clauses must be included in the procurement document(s) to prevent the contractor from inappropriately using or disclosing the information during the course of the contract, agreement, or arrangement and after it has terminated. Contractor must adhere to Business Associate Agreement requirements, as applicable. The Contracting Officer's Technical Representative (COTR) for contracts must monitor contractor compliance to ensure adequate security.

**f. Transfers/Termination of Employees, Students, and Contractors (HIPAA 164.308a3iiC):** When an employee transfers, both the losing and gaining services will adjust menu access as necessary to ensure appropriate minimum-necessary access is granted. When an employee terminates, the **employee's service chief is responsible to ensure that all access is removed, and that Facility Information Security Officer (ISO) and Facility Chief Information Officer (FCIO) are notified within 24 hours of the action.** In both instances, the following must be ensured:

1. **The individual** no longer has possession of unneeded sensitive data media.
2. **The individual** has returned all unneeded keys and access devices as applicable.

3. The individual's status is communicated to the Facility Information Technology Service (FITS) and the Facility ISO to initiate the appropriate actions for the individual's security codes, electronic signatures, menu options, and security keys. The notification of status must be conveyed via the Employee or Student Sign-out Sheet. For situations when the sign-out sheet cannot be utilized, an email message with the concurrence of the responsible service chief or facility senior contracting official.
4. Employee is debriefed on his responsibility to protect sensitive data used on the job from unauthorized disclosure.
5. Appropriate personnel have access to official records created by the terminated employee that are stored on facility systems.

It is the responsibility of the facility senior contracting official to ensure the Facility ISO and the Facility CIO are notified via email of all contractors no longer requiring access to VA computer resources within 24 hours of the termination of a contract.

Occasionally, a termination may be considered an "unfriendly" termination. Under these circumstances, the following procedures may be implemented:

1. Termination of computer system access at the same time (or just before) the employee is notified of his dismissal or upon receipt of resignation. The termination request must be communicated via email to the Facility CIO by the responsible service chief or facility senior contracting official.
2. If applicable, during the "notice of termination" period the user may be assigned to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications. In some cases, physical removal of the employee from the facility may be necessary.

**g. Without Compensation (WOC) (HIPAA 164.308a4i, 164.308a4iiB, 164.308a4iiC):**

Any individual that is not covered under a paid program, but works as a VA employee should have a WOC status. Access granted to these individuals shall be limited to non-sensitive, read-only data whenever possible. These individuals must be supervised if granted access to IT systems or data. All access requests for non-employees, (i.e. Volunteers, WOC, work Study Students) shall be routed through the facility ISO for review and concurrence. Compensated Work Therapy (CWT) workers are NOT considered employees of the United States for any reason and CANNOT legally be granted access to patient information. Allowing CWT patients/workers access to patient information is a violation of the Privacy Act, 5 U.S.C. 552a, and VA medical center staff can be held personally liable under the law. Patients are not permitted to utilize the Internet via the VA Network.

**h. Responsibility Coverage/Cross-training (FISMA 6.1.6):** Employees will be cross-trained in other facility roles to ensure responsibilities are covered in order to continue

facility operations during other employees' scheduled time off. Mandated vacations, as well as cross-training, are encouraged to provide additional security controls.

***2.0 Separation of Duties (HIPAA 164.308a3ii, 164.308a3iiA, 164.308a4ii, 164.308a4iiB; FISMA 6.1.1, NIST 800-53 AC-5)***

**Policy:** The Facility shall ensure a separation of duties methodology is enforced for each information system. Supervisors must ensure a separation of duties so that critical functions are divided among different individuals.

**Procedure:** Supervisors must analyze the duties performed by their employees, identify incompatible duties, assign incompatible duties to different individuals or groups, and verify that users only have the system privileges that are needed to perform their assigned duties (least privilege). The ISO will help ensure that separation of duties issues are identified and appropriate actions taken to correct any conflicts. This type of control must ensure that a single individual cannot subvert a critical process. Supervisors should ensure that a single individual does not perform combinations of functions including, but not limited to:

- Data entry and verification of data;
- Data entry and its reconciliation to output;
- Input of transactions that may result in a conflict of interest, fraud, or abuse (e.g., input of vendor invoices and purchasing and receiving information); and
- Data entry and approval functions.

Some examples of this principle within the facility include:

- The same individual should not enter and authorize a purchase order;
- The same individual should not request a user account and also create the account in the system; and
- The system administrator should not be the one to conduct the audits/reviews of the system he/she is administering.
- The ISO should not be a system administrator.

***3.0 Physical Security Controls (HIPAA 164.310a2ii; FISMA 7.1, 7.2.1, 8.2, 10.1, NIST 800-53 PE)***

**Policy:**

The Facility will implement physical and environmental security controls to protect systems, buildings, and related supporting infrastructures from individual and environmental threats.

**Procedure:**

- a. **Physical access (HIPAA 164.308a7iiB, 164.310a1, 164.301a2ii, 164.310a2iii):**



Access to locations in the Facility that contain equipment or data critical to the information infrastructure shall be limited to authorized Office of Information and Technology (OI&T) personnel. The Facility CIO approves, maintains, and reviews annually a list of personnel with authorized access to these areas. These locked locations include, but are not limited to:

- the computer room
- data/telecommunications closets
- telephone switch rooms (PBX)
- the main telecommunications demarcation point
- IT storage areas
- IT technician work areas

Direct physical access to these locations will be limited to authorized OI&T staff designated by IT management. All other entry into these areas will be strictly prohibited unless authorized and accompanied by IT staff for maintenance purposes. Access to areas that have co-located equipment, which is managed or supervised by a department other than IT, will be coordinated with authorized IT staff.

Entrance doors to sensitive areas shall remain locked unless necessary to open for deliveries or maintenance of equipment. All entrances to sensitive areas also will have available a sign-in/sign-out log for tracking individuals entering these areas. Physical access is controlled to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. All visitors, contractors, maintenance, and housekeeping personnel are required to establish pre-planned appointments with IT prior to receiving access to sensitive areas. Visitors to restricted IT areas will be monitored and escorted. The Facility maintains a visitor access log that minimally includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. The Facility CIO reviews these access logs regularly; not less than annually.

A list of individuals who are assigned a security code or key to access these sensitive areas will be maintained by Facility CIO and the facility Police. These logs will be reviewed periodically, not less than annually, by the ISO and IT management for discrepancies and follow-up actions. The Facility monitors real-time intrusion alarms and surveillance equipment. The Facility also employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

Physical access to storage media containing sensitive data shall be secured by locks and other access controls based on the highest FIPS 199 security category of the information recorded on the media. Removal or movement of the media within the facility is authorized and logged as applicable. Removal or movement of media outside of the

facility must follow all applicable VA, VHA, Network 4 and local directives regarding who can transport and how the media can be transported and stored.

The Facility secures keys, combinations, and other access devices and inventories those devices annually. Changes to combinations and keys occur (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. After an emergency-related event, re-entry is restricted to authorized individuals only.

Emergency access to sensitive areas will be coordinated by facility Police and require Police escorted entry, as appropriate. Facility Police will maintain a log of emergency access and submit a follow up report to IT Chief/CIO. IT management will provide the facility's Chief, Police and Security Services, and the disaster emergency coordinator a list of names of IT individuals who would need access to the facility in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

All members of the workforce are required to wear ID badges for physical access.

Physical security reviews will be conducted and documented by the facility ISO on an annual basis as part of the annual review of the System Security Plans. These reviews will help analyze any new or existing physical security vulnerabilities. Corrective measures will be taken, when appropriate. Physical security reviews conducted by Police and Security Service will be forwarded to the ISO, when applicable.

Maintenance records will be kept to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

**b. Work Area Security; Hardware, Software, and Data Concerns (HIPAA 164.308a5i164.310c):**

1. All employees are responsible for protecting the IT equipment located within their work areas.
2. Government owned equipment is for official use only.
3. Employees are required to implement physical safeguards for all workstations that access protected health information.
4. Employees will log-off of IT systems when leaving work areas and/or invoke a password protected screen saver.

5. Employees will protect data contained on printouts and other media by keeping sensitive data in locked files or cabinets when not in use, and dispose of sensitive data through shredding or other approved disposal methods.
6. To the extent possible, computer monitors will be positioned to eliminate viewing by unauthorized personnel. When computer monitors cannot be positioned to eliminate viewing by unauthorized personnel, the deployment of a CRT privacy screen, which allows viewing only from straight-on, will be used.
7. The use of screen savers, with password protection set at 15 minutes or less, is recommended where applicable in the facility. Users must protect their screen saver passwords. Users will not use function keys or scripts to store passwords or other sensitive information.
8. Supervisors are responsible for keeping their employees informed of proper procedures for fire safety, removal of equipment from medical center premises, protection of equipment and information, and reporting theft of VA assets.
9. Supervisors are responsible for ensuring appropriate measures are taken to protect workstations and other peripheral equipment located within their areas of responsibility from misuse, theft, or unauthorized use.
10. Classes of workstations that have specific functions (such as Data Innovations, Rals Plus, PACS etc.) should have their own set of user security controls and requirements.

**Hardware Concerns:**

1. Hardware modifications shall be strictly controlled and must be performed under the supervision and authority of IT personnel.
2. Users should be certain that the technician(s) performing maintenance is authorized by IT. Additionally, circuit boards or components should not be removed without the express approval of IT. Users are expected to challenge anyone not complying with this procedure.
3. VA Handbook 6500 prohibits the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.
4. Information technology systems or devices not specifically purchased or authorized by IT management are prohibited from being connected to the facility Network or any other IT resource. This includes, but is not limited to, medical systems, software applications, zip drives, "thumb" drives,

laptops/notebooks, PDA's, handheld portable devices, CD burners and printers. IT will not support any system or application not approved through the national IT Tracking System and IT management. Furthermore, IT is authorized to remove from the Network or IT resources, any system or application that does not meet national and/or local purchasing or security requirements.

5. Only IT will move computer equipment from one physical location to another.
6. When appropriate, all sensitive data will be backed-up and secured prior to moving equipment such as servers and mainframes.
7. The Facility controls information system-related items (i.e. hardware, firmware, software) entering and exiting the facility and maintains appropriate records of these items. Supervisors and managers, following Acquisition and Material Management Service (A&MM) property rules and regulations and VA Handbook 6500, shall control the removal, loan, and inventory of IT equipment from the facility for use off-site.
8. Rooms where hardware is located will be secured, or lockdown systems installed to secure the equipment to a table or desk.

**. Data Concerns:**

1. Securing Sensitive Documents: Forms and other types of printed output produced by any computer system will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data should be labeled as such, stored in locked cabinets or desks, and disposed of properly by shredding or placement in specially marked containers. All employees are responsible for retrieving all printed outputs they request from printers or facsimile machines. Information that it is in public view or to be sent outside a secure location will be labeled appropriately.
2. The Facility controls information system media (paper and electronic) and restricts the pickup, transfer, and delivery of such media to authorized personnel.
3. The “double envelope” method is an approved procedure used to transmit sensitive documents. Documents are sealed in the inner of two envelopes and both envelopes shall be addressed to the recipient. The inner envelope shall also display the name and address of the sender, the statement “TO BE OPENED BY ADDRESSEE ONLY” and instructions for contacting the local ISO if it is found to be opened upon receipt. The outer envelope shall also be sealed.

**Software Concerns:**

1. **Software Licensing:** All software installed on the facility's workstations shall be installed by and registered with IT. Approval must be granted by the Medical Center Director before an individual can use personally-owned software on any VA computer system. Use of pirated or illegally obtained software on any VA computer system is strictly prohibited. To ensure compliance with software copyright and licensing agreements, not less than annually, IT and facility ISO shall conduct computer audits. Pirated software found during these audits shall be immediately removed and reported to IT, the facility ISO, and VA SOC in accordance with the VA Incident Reporting policy.
2. **Security Patching and Virus Protection:** All devices that connect to any Network 4 information systems, either on site or from a remote location, must be updated with the latest security patches and virus protection as they are distributed. Medical devices under FDA control must have patches tested and approved prior to implementation. Due to this security risk, all medical devices must be placed on an isolated Virtual Local Area Network (VLAN).

Employee will not advertise on items on the VA intranet without the facility Director approval.

***Requests for Information*****Request Background**

Information contained in the DG Security Log File is covered under VistA, 79VA19, System of Records, and both the Privacy Act and Freedom of Information Act (FOIA). The information is maintained in the VistA computer system and is retrievable by an individual name or unique identifier (social security number).

**Requests must be Documented**

Title 38 CFR §1.526 requires requests for copies of any records in the custody of VA to be furnished in writing. (VA Form 70-3288 Request For and Consent To Release Of Information From Claimant's Records, other VA Form, or a locally developed document may be used). The VA Form 3288 is available at <http://www.va.gov/forms/internal.asp>, or from your local Release of Information department. The written request should contain the name and social security number of the individual on whom the log pertains, reason or purpose for which the copy of the log is requested, dates of the log requested, and signature of the requesting

individual. Requests from individual third parties will require the prior written consent of the person to whom the log pertains. For example; Mrs. John Doe is asking for information on who accessed Mr. John Doe's record, Mr. John Doe has to provide written consent that Mrs. Doe may request the information.

### **Requests from VA Employees**

Written requests from VA Employees for copies of the log pertaining to their records will be directed to the ISO. The ISO will then view or print out a listing of who has accessed the employee's computerized record. The listing will include the name of the individual accessing the record, the menu used, the date, and the time of access. The employee is authorized to have a copy of the information pertaining to their record pursuant to the Privacy Act, 5 USC 552a(d)(1). The ISO must maintain a file of all written requests for information from the DG Security Log File.

If the employee suspects inappropriate activity, the ISO will contact the supervisor of the employee making the alleged inappropriate access to the individual's record, and proceed with the facility's local procedures. The VA employee that is alleging an inappropriate access should be instructed by the ISO not to contact any individual listed on the log to determine the reason for their access to the record due to the possible negative consequences to the investigation.

The supervisor should notify the ISO of their findings concerning the alleged inappropriate access (was it appropriate or has a violation occurred), and that any appropriate personnel actions have been taken. This information should be included in the incident file documentation. Information given to the ISO regarding any personnel actions taken does not need to be specific, (i.e. written reprimand, verbal counseling etc.) only that the supervisor has taken some type of personnel action as recommended by Human Resources. It is not the responsibility of the ISO to recommend what type of personnel action should be taken, that is the role of Human Resources.

The ISO is responsible for contacting the employee that alleged the inappropriate access to report the findings of the investigation. (Susie in the example below).

*For example, Employee Susie asks the ISO for information on who has accessed her record. On the Log Susie notices that her coworker Fred has accessed her record. Susie should not contact Fred and ask him what he was doing in her record. The ISO contacts Fred's supervisor and provides him/her with the information on the alleged violation. It is up to Fred's supervisor to determine if a violation has occurred. If a violation has occurred it will also be up to Fred's supervisor to administer any appropriate personnel action and notify the ISO that a violation has occurred and appropriate personnel action has been initiated.*

If the ISO disagrees with the findings of the supervisor (whether a violation has occurred or not) the ISO would address the issue with the next higher level of the

chain of command at the facility (the supervisor's supervisor). If the employee is not satisfied with the results of the investigation the employee may elevate the situation to a higher level. The ISO is not responsible for directing the employee to the avenues available to them, only to provide documentation if requested by individuals at the higher level (i.e. Medical Center Management, IG, Regional Counsel, EEO, etc).

### **Requests from Veterans**

The recommended process for a request from a veteran is listed below. A request from a Veteran (that is not an employee) should be forwarded to the ISO through the Patient Representative or equivalent. The ISO will investigate as appropriate and provide information directly to the Patient Representative. If the veteran's computerized record has not had the Security Level modified to Sensitive, there will be no record of accesses to that specific record. Modification of the Security Level for this patient's record, to allow review at a later date, should be discussed with the patient by the patient representative, and a determination made based on the local process that has been developed. For Example, A veteran is being treated in the Mental Health department and currently involved in a child custody suit. The veteran is concerned that the medical information would be detrimental if used against him in the suit. His ex-sister-in-law is a nurse at the medical center and he is afraid she will give her sister (his ex-wife) information to help with the case. The veteran's record is currently Non-Sensitive, but could be modified to Sensitive, to track who accesses his record in the future. The Patient Representative will handle communications from and to the patient. The patient should be advised that they should not contact any individual directly concerning the need for access to their record due to the negative impact this could have on the investigation. All concerns should be directed to the Patient Representative. The Patient Representative will forward suspected incidents to the Information Security Officer for investigation. The ISO will investigate and report findings to the Patient Representative who will then contact the patient. If the patient is unhappy with the results of the investigation the patient may elevate the situation to a higher level as designated by local and/or national policies. The ISO is not responsible for directing the patient to the avenues available to them, only to provide documentation if requested by individuals at the higher level (i.e. Medical Center Management, IG, Regional Counsel, EEO, etc).

### **Requests from Third Parties**

Requests from third parties (any individual other than the person to whom the log pertains), including non-VA investigative bodies (i.e. GAO) will be directed to the ISO through the facility medical center management. A record of the release of information for FOIA reporting purposes is required for all non-VA third party requests. If the individual requesting the information is a VA employee (i.e. IG) and the information is required in the performance of their official duties, FOIA reporting is not required.

**Requests from VA Management**

Request from VA Management will be directed to the Information Security Officer. A supervisor may obtain information concerning one of their employees in accordance with the Privacy Act, 5 USC 552a(b)(1). Requests from VA employees for this information in the performance of their official duties (i.e., supervisor investigating inappropriate behavior) do not require a written request or tracking for Privacy Act reporting purposes. However, at the facilities discretion, a local policy may be developed requiring that all requests be in writing.

**Privacy Act Reporting**

The Privacy Act requires VA to keep an accounting of disclosures or copies of records provided to individuals to whom the records pertain and to non-VA third parties. Since the Security Log is part of the VistA (79VA19) System of Records a list of who (other than VA employees in the performance of their duties) has received a copy of the log must be maintained for reporting purposes. The number of disclosures could be calculated based on the written request forms or by the development of a manually maintained log. The number of disclosures will need to be included in your facility's Annual FOIA Report. Near the end of each fiscal year, the VHA FOIA Office issues a directive outlining the reporting requirements for the Annual FOIA Report. The facility FOIA Officer or Chief, Health Information Management Service (HIMS) compiles the data for this report.

**c. Physical Controls:**

- 1.The computer room is located in the center of the building (no windows).
- 2.The computer room's construction is of solid fire-resistant walls that run to the true ceiling.
- 3.The number of doorways into the computer room has been kept to a minimum.
- 4.Unused keys or other unassigned entry devices must be accounted for and adequately secured. The codes will be changed at least quarterly for those areas within the facility that utilize entry codes.
- 5.Annual key inventory will be conducted and records will be available for review.

**d. Environmental Controls (HIPAA 164.308a7iiC, 164.310a2i; FISMA 7.1.12 – 7.1.19):**

1. Fire Safety: The responsible ISO works with the responsible facility services to ensure that appropriate fire safety mechanisms and preventive measures are in place to adequately



protect the facility's data and IT assets. Mechanisms may include, but are not limited to: fire detection systems, a portable fire extinguisher placed at each end of the room, smoke detectors, automatic sprinkler systems, fire fighting equipment, regular maintenance of fire extinguishing equipment, and training of personnel in fire safety procedures and use of fire extinguishers. Fire suppression and detection devices/systems activate automatically in the event of a fire and provide automatic notification of any activation to the facility and emergency responders.

2. **Electrical Outages:** Engineering will ensure that appropriate steps are taken to assure that the quality and reliability of electric power is satisfactory for the facility. All electrical maintenance work will be coordinated with IT to avoid inadvertent shut-off of computer room, environmental systems, or communications power. All electrical power distribution equipment will be adequately protected physically against accidental damage or sabotage, and access to electrical equipment rooms or closets will be controlled. The facility will provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. The facility will also provide a long term alternate power supply that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
3. **Emergency Shutoff:** The Facility has provided the capability in the IT area of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.
4. **Emergency Lighting:** The Facility maintains automatic lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.
5. **Environmental Monitoring:** To control the temperature and humidity, and detect the presence of water in the computer room, appropriate recording equipment is installed and monitored. Facility CIO is responsible for providing temperature and humidity ranges that are compatible with computer equipment specifications. Water sensors are utilized to ensure detection and immediate notification to appropriate staff. Master shutoff valves are accessible, working properly, and known to key personnel.

#### **4.0 IT System Hardware and Electronic Media Sanitization and Disposal (HIPAA 16 4 .310d1; FISMA 8.2.0, 3.2.11 – 3.2.13, NIST 800-53 MP-6, 7)**

##### **Policy:**

The Facility shall follow the media sanitization procedures for fixed electronic media as outlined in VA policy. These procedures ensure that fixed electronic media are

appropriately sanitized or destroyed; the action has been documented; and all VA data is protected to prevent subsequent disclosure when IT equipment containing sensitive data is surplus, donated, or otherwise removed from VA control where the data could be exposed to unauthorized individuals.

**Procedure:**

Excessing/Redistributing IT Equipment/Media (HIPAA 16 4 .310d2i):

The Facility will ensure that the purging or clearing of sensitive data from equipment is accomplished before the equipment is released from custody for disposal. This clearance process must cause the removal of all sensitive data from information systems storage devices or render the data from these systems unreadable. The Facility CIO will be responsible for identifying and training IT staff on VA media sanitization policy and procedures, which include:

1. Overwriting: Data Eraser software by Ontrack is the VA approved over-write technology. Copies of Data Eraser have been distributed for implementation Department-wide. The number of times a overwrite must be performed depends on the storage media and its sensitivity. The Office of Cyber and Information Security requires at least three (3) passes.
2. Degaussing: A degausser that has been tested and approved by the NSA can be utilized. The equipment is periodically tested to ensure correct performance. When a degausser is not available, OCS has a national contract to sanitize and destroy hard drives that can be utilized.
3. Destruction: If a degausser is not available, media can be destroyed using the following methods: a) destruction by smelting (to melt or fuse, returning to a liquid state) at an approved metal destruction facility; b) destruction by pulverization or disintegration (crushing or grinding, reducing media to very small particles) at an approved metal destruction facility.
4. Documentation: VA Form 0751, Information Technology Equipment Sanitization Certificate, must be properly completed, attached to the proper turn-in documentation, and submitted through proper channels for all information technology (IT) equipment, which has the capability of storing information that is turned-in through the Acquisition and Material Management (A&MM). Other IT equipment and electronic storage media containing sensitive data that is not required to be turned-in through A&MM Service is still subject to sanitization procedures prior to disposition or re-use in accordance with NSA/Central Security Service Media Declassification and Destruction Manual procedures.
5. Turn-in: At the time of turn-in, the CMR official will certify to A&MM Service that the data has been removed or made unreadable. The certification will identify the FIP

item(s) cleared and the identity of the certifier (user/CMR official). No FIP equipment will be excessed, transferred, discontinued from rental/lease, exchanged, or sold without compliance with this requirement.

6. The ISO will audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

## **5.0 Mobile/Portable/Wireless Systems (FISMA 7.3, NIST 800-53 AC-19)**

### **Policy:**

Network 4 (1) establishes usage restrictions and implementation guidance for portable and mobile devices and wireless; (2) documents, monitors, and controls the device access to the VA's Network and (3) follows all provision set forth in VA Handbook 6500. Facility CIO should authorize the use of portable, mobile and wireless devices. Mobile, portable and wireless systems should be protected commensurate with the sensitivity of the data stored on them. Mobile, portable and wireless devices will follow VA guidelines regarding system hardware and electronic media sanitization and disposal.

**Procedure:** Employees will not store sensitive data on laptops or other portable devices without encryption. Mobile and portable systems will be stored securely when not in use. Supervisors must ensure users understand their responsibility to securely store all portable systems such as laptop computers, notebook computers, PDA's, handheld devices, wireless telephones and removable storage media devices when they are not in use.

Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to any VA Network without first meeting the VA's and the facility's security policies and procedures. These include scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless). Non-VA systems (any system that is not owned by the VA; e.g., personal home computer) are not permitted to connect and access any VA computer system or data without the required waiver.

Wireless devices can pose a significant security risk to the organization due in part to unique vulnerabilities of the wireless extensions to the Network located outside of the physical confines of the controlled area. To minimize the risk, the following measures shall be implemented.

- a. Strong authentication, non-repudiation and personal identification are required for access to VA systems in accordance with current VA directives and guidance. Identification and authentication will be implemented at both the device and Network level.

- b. Encryption of data transmitted to and from a wireless device is required.
- c. Wireless devices must meet and be kept up-to-date on the latest anti-viral and software/security patch remediation as applicable.

It is recommended that all portable/mobile devices have the anti-virus software, OS and software/security patches updated monthly.

All VA employees, contractors, business partners, and any person who has access to and stores VA sensitive information must have permission from a supervisor and ISO to use removable storage media/devices to store sensitive information.

In order to ensure the protection of sensitive information, all removable storage devices that connect to VA's resources via USB ports (i.e. thumb drives, MP3 Players – iPods, Zunes, and external hard drives) must be encrypted with FIPS 140-2 certified encryption.

Similarly storage media such as CDs/DVDs that contain VA sensitive information must be adequately protected with FIPS 140-2 certified encryption.

### **Thumb Drives**

All Department staff, contractors, business partners, or any person who has access to and stores VA sensitive information must have written approval from their respective VA supervisor and ISO before sensitive information can be removed from VA facilities/operating units.

VA sensitive information, to include all sensitive information entrusted to VA, must be in a VA protected environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed.

Utilization of personally-owned USB thumb drives within the Department is prohibited. FIPS 140-2 certified USB thumb drives will be procured with VA funding for VA employee utilization, if the need to utilize a thumb drive as an external storage device exists. This must be approved by the individual's supervisor and the thumb drive must be provided by the local OI&T senior representative.

The procurement of thumb drives will be accomplished under the direction and control of OI&T.

VA employees are not authorized to access or store any VA information using a thumb drive that has not been procured and issued by OI&T and they must have written permission to receive and use a VA issued thumb drive.

Non-VA personnel (contractors, business partners, etc.) supporting VA must furnish their own FIPS 140-2 certified USB thumb drives that conform to the published listing of VA approved USB thumb drives. Further, permission must be obtained from a designated VA supervisor before they can be utilized.

The listing of VA approved USB thumb drives is derived from NIST FIPS 140-2, Validation Lists for Cryptographic Modules. This listing can be found on the Information Assurance Web Portal. The link to this portal can be found on the VA Intranet, Office of Information and Technology home page.

To prevent the utilization of unauthorized thumb drive all Network 4 facilities have installed a port blocking software known as sanctuary

## **Sanctuary**

Sanctuary is a product which, when in full operation, will allow us to block devices on a PC. A device, as viewed by Sanctuary, is the same as viewing devices in Computer management. Therefore a device could be a Printer, USB Drive, COM port, CDROM, hard drive, Serial port, etc. The Sanctuary Architecture is set up whereby each Network has a single "Application Server". This application server has an install of Sanctuary which connects to a single database at the RDPC. Each VISN then is configured with two failover Sanctuary servers to fall back to in the event of a failure of a single server. This provides redundancy and failover within the architecture.

The Network 4 Sanctuary servers are also configured to apply restrictions and approval on devices to end users and end PC based on Policies. The Policies within Sanctuary that are setup in Network 4 have the following features

Sanctuary has a Single Policy across all ten facilities within Network 4. This means that if a Compaq USB device is allowed at one facility, the same policy gets applied to the other 9 facilities.

Policies within Sanctuary are set up so that devices are blocked unless otherwise approved. This means that once we are in 'blocking mode' if a device comes on line that is seen as a 'removable storage device' by Sanctuary, it will be blocked by default.

Two USB Removable Storage Devices have been approved for VA use. The ONLY two approved USB Removable Storage Devices are Kangaroo and Meganet "thumb drives". VA sensitive information may not reside on other non-VA owned Other Equipment (OE) unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO.

The non-VA systems or devices must conform to, or exceed, applicable VA security policies or are specifically authorized by official VA policy. Users of remote systems must follow all policies and procedures outlined in this policy.

The local OI&T Chief /CIO and supervisors will authorize the use of portable, mobile and wireless devices within their operating unit.

Two-factor authentication, (where one of the factors is provided by a device separate from the computer gaining access) is required for remote access to VA systems.

All remote systems (VAGFE and OE) must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA-approved configuration. Software must be kept current, including all critical updates and patches. The local facility OI&T office will provide and maintain the software for VAGFE. Users of waived OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

All devices used to transmit and store VA information outside of VA's protected environment must use FIPS 140-2 approved encryption. This includes laptops and thumb drives and other removable storage devices.

Mobile and portable systems will be stored securely when not in use. Supervisors must ensure users understand their responsibility to securely store all portable systems such as laptop computers, notebook computers, PDA's, handheld devices, wireless telephones and removable storage media devices when they are not in use and whenever they are in an unsecured environment.

VA employees, contractors, subcontractors, and volunteers must immediately report to his or her VA supervisor and the local ISO any incident of theft, loss, or compromise of any VA sensitive information, VA equipment or device, or any non-VA equipment or device used to transport, access, or store VA information. The ISO will promptly report the incident (within one hour) to the VA-NSOC in accordance with the OI&T Incident Management procedures.

Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to any VA network without first meeting the VA's and the facility's security policies, procedures, and configuration standards. These include scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

Mobile, portable and wireless devices will follow VA policy regarding system hardware and electronic media sanitization and disposal.

## **Blackberries**

Blackberry wireless remote service can be used within VISN 4 if the following conditions are met:

1. Blackberry device, server, and service must be approved by the Information Security Officer.
2. Only VA-approved Blackberry e-mail service providers will be used.
3. Only the Blackberry enterprise server e-mail redirector will be used, and it must be configured for triple data encryption standard.
4. Workstation-based redirectors will not be used for wireless e-mail systems.
5. The Blackberry redirection server must be configured to disable peer-to-peer communications. Blackberry peer-to-peer (pin-to-pin) messaging does not meet VA security requirements.
6. Master keys must be generated from the Blackberry server only, and must be renewed every 30 days.
7. All Blackberries will use the alphanumeric password with a requirement to change the password every 90 days. All passwords will include a number, letter and special character
8. The Black berry security timeout will be set to 15 minutes of non-activity

**Internet Gateways –**

The Operating Unit will use the VA approved national gateways to access the Internet. These gateways are configured to restrict information flow based on an approved rule set. Users will use the Internet in a secure manner. All users must adhere to the national and local Internet access and usage policy when accessing the Internet and understand that Internet activity is monitored. NO PATIENTS are permitted to utilize the VA network for connection to the internet.

**External Business Partner Connections** - Data communication pathways from VA facilities to non-VA business partners that cannot pass through the One-VA Internet gateways must be fully documented and must have OI&T Chief/CIO and ISO approvals. These connections must be managed and coordinated with and by the VA NSOC.

**6.0 Contingency Planning (HIPAA 16 4 .308a7i; FISMA 9.0, 12.1.8, NIST 800-53 CP)****Policy:**

The Facility will establish, implement, review, and disseminate, as needed, policies and procedures for responding to an emergency or other occurrence that damages the IT resources that contain or maintain sensitive data.

**Procedure:**

The Facility has developed the following levels of contingency planning to restore normal operations in the event of a service disruption to the facility or system.

**a. Disaster Recovery Plan:**

This plan is the overall facility contingency plan and is coordinated with this site's Emergency Management Office and approved by the facility director. This plan defines the overall contingency objectives and establishes the framework, roles, and responsibilities. The plan will address the scope (to include CBOCs and other remote resources), resource requirements, processing priorities, training, testing, plan maintenance, and backup requirements. Activities involved in this function include conducting an impact analysis, identifying preventive measures, developing a recovery strategy, documenting the disaster plan, distributing the plan to appropriate individuals, training the staff, and testing the plan.

The Facility has an alternate processing site policy that defines the alternate processing site policy and procedures. The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards. The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site. The Facility has identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and has addressed these issues in the disaster recovery plan. This arrangement is documented, reviewed, and approved annually to ensure the plan is still appropriate and that the required resources are available.

The contingency plan must identify the activities that are necessary to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. The recovery strategies must include the sequence of activities as well as detailed procedures for the technical recovery of operations until the system can be reconstituted. The IT contingency plan also documents the following resources required for supporting critical functions: computer hardware and software; computer supplies; system documentation; telecommunications; office facilities and supplies; and human resources.

**Emergency Mode Operation Plans (HIPAA 16 4.308a7iiC):****Service Contingency Plans:**

Written contingency plans must be maintained for each service and should include a means by which routine business operations may continue when computer system capabilities have been eliminated or diminished. Contingency plans should also include procedures for data recovery when the computer systems come back on line. Contingency plans will be consolidated for the Facility to respond to contingencies as necessary for



their IT systems. These plans will be part of the overall facility Disaster Plan. ADPACs and IT staff are responsible for the preparation and accuracy of contingency plans. IT is responsible for prioritizing the critical functions and documenting plans for contingency/recovery of information systems in the event of scheduled or unscheduled downtime. Managers are responsible for the development of their specific components of the contingency plan and ensuring that employees under their management receive annual training on their specific roles and responsibilities. When applicable, simulated events and automated mechanisms are used to train individuals regarding their specific roles and responsibilities.

Any changes to the plan must be fully documented and the members of the contingency planning teams notified of the relevant changes. Each update of the contingency plan will require concurrence of the Medical Center Director or designee, and distribution to the appropriate individuals. Distribution of the plan will be limited to authorized individuals, and a complete copy of the plan will be stored at an off-site location.

#### **System Specific Contingency Plans:**

These plans will outline procedures specific to each system within the facility and will include information such as procedures for shutting down and restoring a system during an emergency, contacts and vendors, and responsibilities during an emergency. The system administrator is responsible for preparing the contingency plan for the system. Distribution of the plan will be limited to authorized individuals and a copy of the plan will be stored with Facility CIO and at an off-site location. Contingency plans are re-evaluated prior to a significant change in the system, but are reviewed at least annually. The plan should be revised to address system/organizational changes or problems encountered during plan implementation, execution or testing. Systems which may pose a high risk and potential magnitude of harm will be re-evaluated more often. Each plan will be documented as part of the certification and accreditation of the system.

#### **b. Electronic Media Backups (HIPAA 16 4 .308a7i):**

##### **Data Back-up and Storage:**

Facility CIO is responsible for establishing, maintaining, and executing written procedures for backup and restoration of production systems. Critical data files and operations are identified and the frequency (daily, weekly, monthly) and scope (full backup, incremental, differential) of file backup are documented. All system security configurations are documented and backed-up. The backups are completed on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged. The location of the stored backups is documented. Backups shall also be verified periodically to ensure that they are complete and contain valid data by using system specific restore functions. A file restore recommended monthly to verify restoration abilities. Documentation should be kept of all restore attempts. Each site

selectively uses backup information in the restoration system functions as part of contingency plan testing.

**Off-Site Storage:**

Each site has identified and initiated the necessary agreements for storage of the site's backup information. Backups are being stored in a secured location away from the facility in order to avoid loss in the event of an accident or malicious incident. The data is labeled, packed, and transported to the off-site storage facility securely. A local risk assessment was completed to determine that the selected site was sufficiently distant from the facility to reduce the risk of the storage location being affected by the same disaster. The priority with which the facility can obtain its back-ups in the event of a catastrophic emergency was considered. The storage facility has controlled access, proper environmental controls, and reinforced concrete or steel beam construction that has been earthquake proofed. Access control to the VA information stored at this location is stringently controlled and periodically tested. Locks and personnel are used to control the off-site storage to prevent unauthorized access. System and application documentation and an up-to-date copy of the contingency plans are also stored securely at this off-site location.

**c. Contingency Plan Testing (HIPAA 164 .308a7iiD):**

To ensure the accuracy and reliability of contingency plans, IT managers and supervisors will conduct tests on the components of the plan for which they are responsible, and will update the components based on evaluation of the results. Tests will have a specific objective such as: determining the availability of needed back-up files, implementation of fire and evacuation procedures, and implementation of manual procedures. The tests will also provide an opportunity for training of key personnel in the proper procedures to be followed in the event of an emergency. Contingency plan testing will be documented and test results reported to the ISO. When applicable, the Facility employs automated mechanisms to thoroughly and effectively test the contingency plan. When feasible, a full recovery and reconstitution of the information systems is used as part of the contingency plan testing.

**Alternate Processing Site**

The Facility has an alternate processing site policy that defines the alternate processing site policy and procedures. The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards. The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site. Recoverall will provide necessary resources within 72 hours for resumption of information system operations for critical mission/business functions. The Facility has identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and has

addressed these issues in the disaster recovery plan. This arrangement is documented, reviewed, and approved annually to ensure the plan is still appropriate and that the required resources are available. The agreement with the alternate site contains priority-of-service provisions.

### **Telecommunications Services**

The Facility has identified primary and alternate telecommunications services to support the information system and has initiated necessary agreements to permit the resumption of system operations as soon as possible. The primary and alternate telecommunications service agreements contain priority-of-service provisions. The alternate telecommunications services do not share a single point of failure with the primary telecommunications services and the providers are sufficiently separated from the primary service providers so as not to be susceptible to the same hazards. Both the primary and alternate telecommunications service providers have adequate contingency plans.

## **7.0 IT System Hardware and Software Maintenance (FISMA 3.1. 4, 10.0, NIST 800-53 CM)**

### **Policy:**

To ensure the integrity of the system, procedures should be in place to monitor the installation, maintenance, and configuration of hardware and software. IT staff are required to implement applicable security updates and patches in a timely manner or as directed by VA SOC.

### **Procedure:**

#### **Configuration Management:**

The Facility utilizes the VA established guides and policies for the proper configuration, setup, and operation of our servers, applications, and desktops. The security settings established by the configurations should be as restrictive as possible. The site reviews the information systems periodically to identify and eliminate unnecessary functions, ports, protocols, and/or services. This process is defined and monitored via a configuration management plan. Vendor-supplied default security parameters must be changed to conform to the VA standards. The ISO will coordinate with system owners, system managers, and IT personnel to identify and implement approved VA policies and guidelines necessary to ensure the compliance of approved configurations for the systems within the facility. System configurations (including links to other systems) will be documented and updated accordingly with any major changes in the system's security plan. The production configuration must be backed-up on a schedule specified by IT, not to exceed quarterly.

The site maintains an inventory of the systems' constituent components. The inventory of the information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture). The Facility updates the baseline configuration as an integral part of information system component installations and employs automated mechanism to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

**a. Change Controls:**

Facility CIO, the ISO, and other specified individuals as needed, comprise the Change Control Board. The Board ensures that changes are documented and tested. The Board monitors changes to the information system and ensures security impact analyses are completed to determine the effects of the changes. If the facility environment necessitates a different configuration for a particular system than the configuration approved by VA, the change request must be documented and evaluated by the Change Control Board. If the proposed change affects the security of the system, the system must be re-certified and accredited by OCS. All changes to the configuration of a system will be documented in the system's security plan. The system owners, system managers, IT personnel, and the ISO will review all VA-NSOC security alerts and take appropriate remedial actions in a timely manner. The Board ensures that access restrictions associated with changes to the system are implemented and monitored. Emergency change procedures are documented and approved by management either prior to the change or immediately after the fact. The Facility audits activities associated with configuration changes to the information systems.

**b. Hardware Maintenance:**

IT schedules, performs, and documents routine preventative and regular maintenance on the components of their information systems in accordance with manufacturer or vendor specifications.

Facility CIO approves the removal of the information systems or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the facility removes all information from associated media using approved procedures. After maintenance is performed on the information system, the facility checks the security features to ensure that they are still functioning properly.

IT maintains a maintenance log for their information systems that includes (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

The site employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

Facility CIO approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis. IT inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications. IT also checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system. IT checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

Facility CIO approves, controls, and monitors remotely executed maintenance and diagnostic activities and assures that the use of remote diagnostic tools is described in the security plans for the systems. IT maintains maintenance logs for all remote maintenance, diagnostic, and service activities and periodically reviews these logs. In addition, for systems categorized as high, the following controls are also required:

- IT audits all remote maintenance sessions, and reviews the audit logs of the remote sessions.
- IT addresses the installation and use of remote diagnostic links in the security plan for the information system.
- Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.

Bio-Med staff for medical equipment and IT staff for other IT equipment maintain a list of personnel authorized to perform maintenance on their systems. Only authorized personnel perform maintenance on the information systems. Maintenance personnel have appropriate access authorizations to the information systems when maintenance activities allow access to sensitive information. When maintenance personnel do not have needed access authorizations, local staff must supervise maintenance personnel during the performance of maintenance activities on the information systems.

Each site obtains maintenance support and spare parts based on service level agreements or contracts.

[VHA VistA] Processing Environments:

- a. **Production:** This is the environment for the processing of official data utilized in the provision of health services to the Veteran in support of the facility-wide mission. The system manager is responsible for production system maintenance and the implementation of mechanisms that address the protection of sensitive data and the processing system, ensuring access controls defined in this policy are in place. The ISO will perform routine monitoring of the production system ensuring adherence to set procedures.
- b. **Development and Verification:** This is the environment for development, testing and verification of program code for the maintenance, modification or enhancement of existing applications, or the development of new applications. The development account is maintained by IT. User access to this account will be granted upon approval by IT. Minimum necessary access controls will be applied in granting these accounts. The distribution and implementation of new or revised software is documented and reviewed. Version control is utilized and all software programs are labeled and inventoried.
- c. **Test system:** This may be an environment used for testing new software applications and revisions. IT is responsible for maintaining the test system. This includes the installation of software packages and necessary patches as they are released and mandated. IT is also responsible for managing test system user accounts. Existing users may receive access to the test system IT staff sponsoring the user. IT will ensure that test account access is appropriate for the user and that it does not allow them access that can compromise the integrity of the test system or compromise the 'mirroring' capability as the mirror of the production system.

**Active Directory (Windows/NT)** test accounts within VISN 4 must be controlled, easily identified, used only for its intended purpose, and disabled/deleted when not in use. Sites must follow guidance provided below:

- All test accounts created must be approved by your supervisor and ISO
- A rules of behavior must be signed and on file for the test account owner
- Uniformed naming convention for new and existing accounts using the following naming structure:
  - First Name = First name of account owner
  - Last Name = Last name of account owner
  - Alias = AAABBBCCCCD\_Testx
    - AAABBBCCCCD = your current NT account name
    - x = number starting at 1, then 2, etc.
    - Example: VHAWBPTestp\_Test1, and additional accounts being VHAWBPTESTp\_Test2
- All test accounts must be disabled or deleted when no longer in use.
- All test account title must be "Test Account for Windows logon and permissions"
- The account owner's phone number must be listed

- Passwords will not be shared
- Utilizing this account as a "Generic Login" is prohibited
- All test accounts will be used specifically for its official intended purpose. Using test accounts for personal use, surfing the web, etc is not authorized
- No exchange accounts should be included in these test accounts as appropriate.
- The account must be set with expiration date not to exceed 90 days.

## **8.0 Data Integrity (HIPAA 16 4 .312c1, 16 4 .312c2; FISMA 11.0, NIST 800-53 SI)**

### **Policy:**

The Facility identifies, reports, and corrects information system flaws. The Facility protects sensitive information from improper alteration or destruction. Local modification of the [VistA Kernel] software security features is strictly prohibited. Additionally, Health Information Management plays a role in maintaining the content, accuracy, and completeness of sensitive data and tracking historical changes to the medical record.

### **Procedure:**

The Facility CIO is responsible for maintaining overall integrity for all IT systems within the facility. A record of modifications to existing [VistA], commercial, or locally-developed software will be maintained. The Facility CIO reviews each system installation of facility-developed new or modified software and restricts and controls access to all program libraries.

The site enforces access restrictions associated with changes to the information system. Willful and intentional modification of VA software processing fiduciary data (e.g., IFCAP, PAID) for illegal or disruptive purposes or for purposes of personal gain is a felony. There shall be no local modifications of fiduciary programs without the approval of the issuing CIO field office. The Facility CIO or designee(s) shall ensure that programs processing fiduciary data have not been modified both prior to receipt and annually after they have been placed into production.

Any local modifications to VA software must be reviewed, tested, approved, and documented by Facility CIO and the ISO. The site will be required to re-certify and accredit the software prior to going into production, if any local modifications to the VA software have the potential to affect the security of the software.

The site protects the integrity of information and information systems through antivirus programs and intrusion detection software. The anti-virus solution is managed both locally and centrally and systems automatically update. Users will not take any action that invites or allows a computer virus to be introduced into any VA computer system. To reduce the risk of viruses, the following procedures will be followed:

Authorized and current anti-virus software will be used and enabled at all times. IT is authorized to disconnect, either physically or logically, any device that is not protected with current anti-virus software.

All new software shall be tested on an isolated computer to avoid damage to working computers if a virus is present.

Downloaded software from the Internet will be scanned for viruses.

Users will be given training which covers the risks that viruses pose to IT assets, common ways that viruses are introduced, how to prevent viruses, and how to detect them, warning signs of the most common viruses, and what to do if a virus is detected or suspected (who to call, when to call).

The site employs tools and techniques to monitor events on the information systems, detect attacks, and provide identification of unauthorized use of the system. Intrusion detection tools are used to identify unauthorized attempts to probe a system, especially attempts to gain unauthorized access. The IT staff and the ISO will work with the VA SOC and Network Command Center (NCC) to monitor VA's Network .

The Facility CIO is responsible for ensuring that adequate software security measures are implemented to verify the access authority of individuals and to protect files from unauthorized or accidental modification, destruction, or disclosure. Local managers or designees are responsible for monitoring compliance with, and ensuring that all employees are following, IT security policies.

Each site receives information system security alerts/advisories on a regular basis and takes appropriate actions.

## **9.0 Security Documentation (HIPAA 16 4 .306; FISMA 12.0, NIST 800-53 SA)**

**Policy:** The Facility ensures that adequate documentation for its information systems and its constituent components are available, protected when required, and distributed to authorized personnel. IT system managers and Facility CIO in conjunction with the ISO must ensure that sufficient documentation is developed and maintained to formalize security and operational procedures for the facility's IT systems.

**Procedure:** In addition to the certification and accreditation documentation (security plan, risk analysis, contingency plan, and testing documentation) the following documentation will be maintained for each system, if applicable:

- a. User manuals for software;



- b. In-house application documentation (application requirements/program documentation, specifications/change control recommendations);
- c. Any vendor-supplied documentation;
- d. Standard operating procedures;
- e. Network diagrams and documentation on setups of routers and switches;
- f. Software and hardware testing procedures and results;
- g. System interconnection agreements;
- h. Hardware replacement agreements; and
- i. Vendor maintenance agreements and maintenance records;
- j. Documentation describing the functional properties and design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

The ISO will conduct annual reviews of security documentation with system owners, system managers, and IT personnel.

## **10.0 Security Training, Education, and Awareness (HIPAA 164.308a5; FISMA 13.0, NIST 800-53 AT)**

**Policy:** VA Handbook 6500 requires mandatory periodic training in computer security awareness and accepted computer practices for all VA employees, contractors, and all other users of sensitive VA information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. The site identifies personnel with significant information system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff) and documents those roles and responsibilities, and provides appropriate additional information system security training.

**Procedure:** Orientation training will be conducted for all new employees in accordance with the New Employee Orientation program. For those individuals who cannot immediately attend new employee orientation, the service will provide basic security awareness training. At minimum, the following computer security awareness basics will be addressed prior to system access and during the orientation training:

- a. Knowing the ISO;
- b. Creating strong passwords and protecting them;
- c. Maintaining confidentiality of information;
- d. Complying with the Privacy Act;
- e. Backing up data and information;
- f. Using e-mail properly and securely;
- g. Using “reply to all” in a manner that will not create a denial of service;
- h. Identifying and reporting computer security related incidents;

- i. Recognizing VA Cyber Security as part of the nation's infrastructure protection;
- j. Recognizing social engineering and defending against it;
- k. Understanding authorized, limited personal use of government equipment and computer resources (employee advertising on VA intranet is prohibited);
- l. Understanding the HIPAA Privacy and Security Rules and the penalties for non-compliance;
- m. Understanding proper disposal techniques for information on computers and portable media; and
- n. Understanding proper workstation use and security.
- o. Monitoring of log-in dates and times in Vista

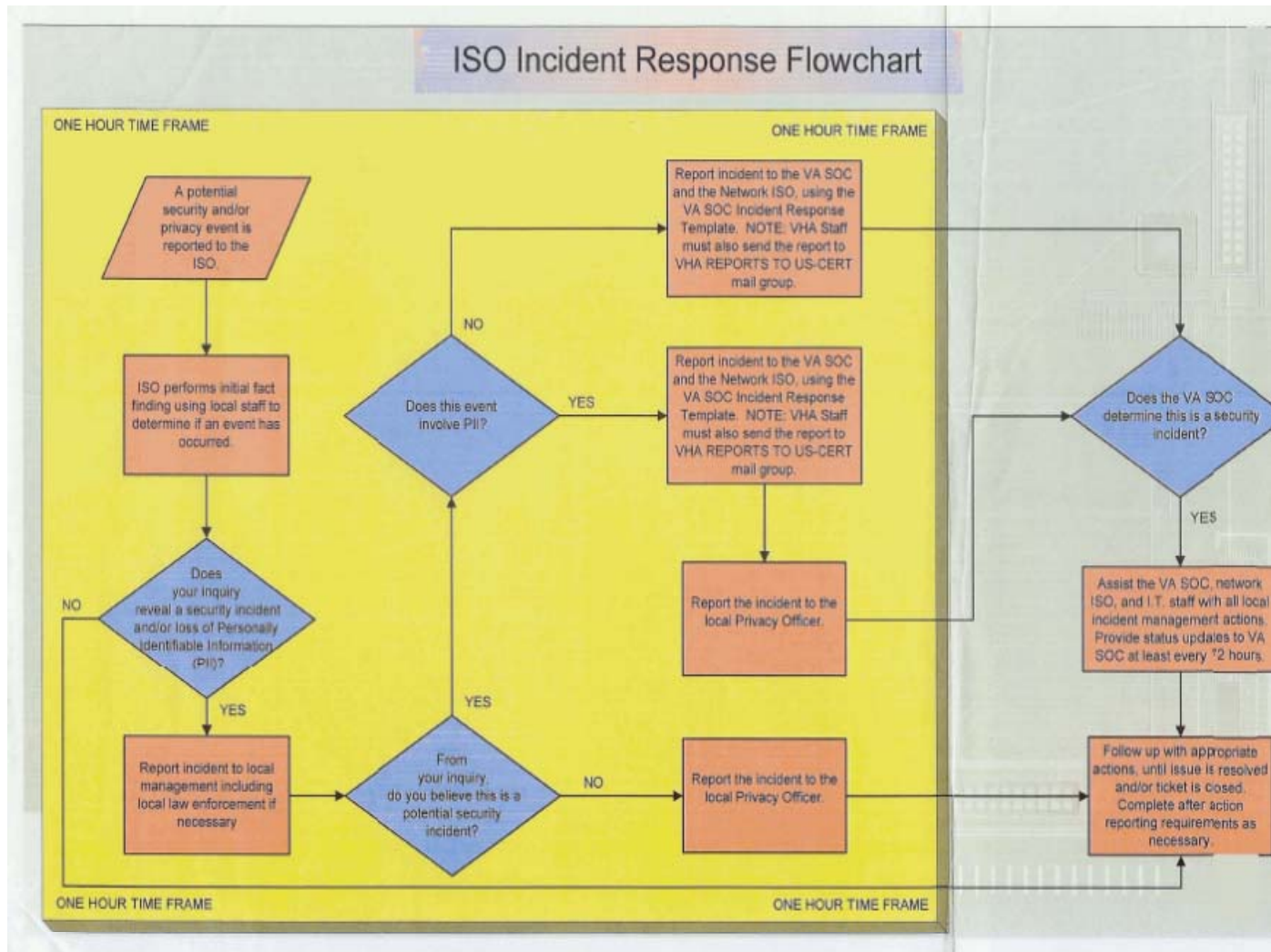
The Facility's workforce will receive security awareness training annually as part of the Mandatory Training Program. Training will be presented to users by either in-house presentations, OCS security awareness web based training, posters, videos, pamphlets, conference calls, and in electronic mail messages as the need to communicate security issues is identified.

All computer security awareness training shall be documented in the training package (i.e., TEMPO or LMS). The ISO will monitor both the basic security awareness training and the role based system security training at their facility and will have access to the training information.

### **11.0 Incident Response Capability (HIPAA 164.308a6ii; FISMA 14.0, NIST 800-53 IR)**

**Policy:** The Facility complies with the VA-NSOC incident reporting policy for all incidents. All incidents related to information security shall be reported to the ISO in accordance with national and local Incident Reporting policy to assure that computer security incidents are detected, reported and corrected as quickly as possible, and with minimal impact. The responsible ISO will also notify the appropriate Medical Center or Program Office management and the Network 4 ISO.

**Procedure:** Users will promptly report any situation that leaves an information system in a less than fully operational state or which violates information security laws or policies (i.e., missing equipment, fraud, virus infection, disclosure, etc.) to the ISO and appropriate management officials. The ISO will utilize the Remedy and FERET system for reporting all incidents to VA-NSOC within one hour of notification. The facility ISO should notify their local Incident Response Team (IRT) in addition to the Network 4 ISO. If incident involves privacy, ISO also notifies the Privacy Officer. ISO will provide updates to VA-NSOC every three days until the incident is resolved/closed.



The ISO will work with management and, if a compromise occurred, members of the appointed investigative team will examine the details surrounding the incident ensuring data and systems are not compromised. The ISO will contact either automatically via electronic mail and/or via phone the VA NSOC to coordinate a response to the incident and to limit the damage. The VA NSOC offers advice and assistance regarding handling and reporting of security incidents. This support resource is an integral part of the organization's incident response capability.

The first report will be preliminary and will include the following information:

- a. Organization in which the incident is first observed
- b. Date of report
- c. Name of person filing the incident report
- d. Point of contact, if different from the person filing the report
- e. Phone numbers of the person filing the report and the point of contact
- f. Email address of the person filing the report and the point of contact
- g. Affected system name and IP address (if known)
- h. Detailed description of the incident
- i. Date and time the incident was first observed
- j. User community affected
- k. Preliminary actions taken

Computer security incidents that fall under the following categories shall be reported:

- a. Circumvention of computer security controls, safeguards, or procedures
  - b. Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of data and information technology resources
  - c. Theft, fraud, or other criminal activity committed with the aid of information technology resources
  - d. Theft, loss, or vandalism of hardware, software, or firmware
  - e. Issues affecting confidentiality, integrity, and availability of data and information technology resources
  - f. Unauthorized downloading or copying of VA information
  - g. Examples of reportable incidents are listed in Attachment E.
- Computer security incidents have many possible consequences that range from slight to catastrophic. Priorities are established to evaluate incidents and determine the best method to manage them. The following 4 priorities shall be used, in the order they are listed, to triage and control computer security incidents affecting the facilities within Network 4:

Priority 1 – Protect human life and safety

Priority 2 – Protect data

Priority 3 – Prevent damage to other categories of info resources, e.g., hardware

Priority 4 – Minimize denial of service

All incidents involving a significant data breach will require activation of the facility or Network Incident Response Team (IRT) as appropriate. A significant data breach is defined as an incident where the loss of personally identifiable information (PII) is more than 20 veterans and/or VA staff. The following are examples of a significant data breach: loss of more than 20 veteran names with or without any other identifying information; loss of a personal computer (PC) or laptop that is not encrypted and stores PII with records for more than 20 veterans and/or staff; loss of external storage media such as an external hard drive, CD, DVD, tape or thumb drive where PII for more than 20 veterans or staff is stored; and loss of multiple paper records for more than 20 individuals that leave VA possession and control.

VA Police will be notified to determine if the incident warrants a criminal investigation. This includes, but is not limited to, theft of computer equipment or software, destruction of or tampering with government equipment, illegal Internet activity, electronic mail that poses a threat to patients or staff and falsifying or stealing information contained in VA systems. Police investigative procedures will be followed to determine if criminal activity occurred. Pending preliminary investigation results, the Chief of Police or designee will work with the ISO to meet VA-NSOC reporting requirements.

Corrective action will be documented following all reported incidents prior to closing the incident report.

The Incident Response Team is responsible for adhering to the national policy and procedures governing incident resolution for data breach mitigation.

Incident Response Team (IRT) will include the Privacy Officer, ISO, IT staff and Police staff for response to significant data breaches.

Once the VA-NSOC receives an incident report, they will work with the reporting facility, the facility/ VISN Network 4 ISO and, if necessary, the Network 4 ISO providing electronic mail, facsimile, or telephone support and coordination to facilitate the following actions:

- a. Properly coordinate the incident with all necessary parties
- b. Identify, isolate, and analyze the incident
- d. Ensure the integrity of critical systems
- e. Maintain and restore data
- e. Maintain and restore service
- g. Avoid escalation and recurrence
- h. Avoid negative publicity
- i. Identify the source of the incident, and report it to the proper authorities

A complete incident report, including a full description of the final incident resolution shall be submitted to VA-NSOC, appropriate Medical Center or Program Office

management and to the Network 4 ISO no more than five business days after the incident is resolved.

VA-NSOC shall be responsible for supplying incident reports to the VA CIO Information Security Officer, and to the primary organizational contact for the affected organization.

VA SOC may also alert the Facility of suspicious or malicious activity when such activity has been detected by the National Security Operations Center (NSOC). The ISO will resolve the matter according to VA-NSOC's Rules of Engagement.

Through the VA-NSOC Remedy system, the ISO will complete a risk assessment using the Formal Event Review Evaluation Tool (FERET). If the FERET score result is medium or high risk, it will be necessary to activate the local Incident Response Team (IRT) and complete a FERET risk assessment every three days until the score stabilizes. The IRT will follow the VA OI&T Incident Resolution for Data Breach Mitigation policy and procedures.

The VA SOC will provide the technical guidance, advise vendors to address product/software related issues, and provide liaisons to legal and criminal investigative groups as needed. The VA SOC will also ensure that, if appropriate, the related information will be shared with owners of interconnected systems, FedC VISN, and other local law enforcement.

The site will also:

- Train personnel in their incident response roles and responsibilities in respect to information security and provides annual refresher training. The training incorporates simulated events to facilitate effective response by personnel in crisis situations and employs automated mechanisms, when applicable, to provide a more thorough and realistic training environment.
- Test the incident response capability for their information systems annually using facility defined tests and exercises to determine the incident response effectiveness. All tests are documented and automated mechanisms are used when appropriate to track and document information system security incidents on an ongoing basis.

**REPORTABLE INCIDENTS – VA-NSOC**

	<b>Reportable Incidents</b>	<b>VA-NSOC One Hour Reporting Requirement</b>	<b>Privacy Tracking Violation System Reporting</b>
<b>1.</b>	Using another person's individual password and/or account information	X	If includes PII
<b>2.</b>	Failure to protect passwords and/or access codes (i.e. sharing individual codes; taping to equipment to avoid memorizing)	X	If includes PII
<b>3.</b>	Accessing a patient record for other than a "need to know" reason	X	X
<b>4.</b>	Asking unauthorized personnel to access your personal record/data	X	
<b>5.</b>	Unauthorized personnel accessing a co-workers record in response to their request	X	X
<b>6.</b>	Leaving a workstation signed on/unattended prior to activation of screensaver or failure to log off.	X	If includes PII
<b>7.</b>	Unscheduled system downtime	X	
<b>8.</b>	Unauthorized use of external computer connections (i.e. modems)	X	
<b>9.</b>	Installation of unauthorized software (screensavers, games, etc.)	X	
<b>10.</b>	Indication of computer virus	X	
<b>11.</b>	Illegal reproduction of sensitive data	X	
<b>12.</b>	Inappropriate disposal of patient data	X	If includes PII
<b>13.</b>	Falsifying data (patient, financial, employee, mission critical, etc.)	X	X
<b>14.</b>	Disclosing patient information with unauthorized personnel; failure to safeguard confidential data	X	X
<b>15.</b>	Theft of computer equipment or software	X	If includes PII
<b>16.</b>	Inappropriate use of software, such as illegal copying of licensed computer software, intentional introduction of computer viruses, etc.	X	
<b>17.</b>	Inappropriate use of the Internet	X	
<b>18.</b>	Inappropriate use of electronic mail	X	If includes PII
<b>19.</b>	Misuse or defacing government equipment	X	
<b>20.</b>	Destruction or tampering with government equipment	X	

## Technical Control Procedures

### 1.0 Identification and Authentication (HIPAA 164.312a1, 164.312a2, 164.312d; FISMA 15.1.1, 15.2.2, NIST 800-53 IR)

**Policy:**

The Facility has implemented system controls to uniquely identify users to the system. Each user ID will be associated with a unique password to authenticate the individual/entity.

**Procedure:**

User access will be controlled and limited based on positive user identification. Authentication mechanisms support the minimum requirements of access control, least privilege, and system integrity for all platforms.

The following are the VA's information system account and password management procedures (HIPAA 164.312a2i, 164.312a5iiD):

- a. **Access Codes and User IDs:** The assignment of access codes and user IDs will follow VA naming conventions per Appendix F of VA Directive 6500 Handbook:

Passwords must be created consistent with the following criteria:

- 1 Passwords must have at least eight (8) non-blank characters;
- 2 It must contain characters from three of the following four categories:
- 3 English upper case characters (A...Z);
- 4 English lower case characters (a...z);
- 5 Base 10 digits (0...9); and
- 6 Non-alphanumeric, special characters (For example, !,\$#%).
- 7 Six of the characters must not occur more than once in the password (e.g., 'AAAAAAA1' is not acceptable, but 'A%rm2g3' and 'A%ArmA2g3' are acceptable); and
- 8 Passwords must not include any of following: vendor/manufacture default passwords: names (e.g., system user names, part or all of your account name, family names), words found in dictionaries (i.e., words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468). Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, Demo, and TEST, must be replaced immediately upon implementation of a new system.
- 9 Systems or applications that have multiple passwords for different levels of access or authentication must have unique passwords for each level.
- 10 Passwords must be protected to prevent unauthorized use. Specifically:



- 11 Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit system security plan. Once shared, passwords must be changed as soon as possible. Group passwords (i.e., a single password used by a group of users) must not be used without some other mechanism that can assure accountability (such as separate and unique Network User IDs).
- 12 Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized. Group passwords must never be re-used.
- 13 Passwords that need to be shared because of an overriding operational necessity, as well as group passwords, cannot be used to control access to other Information Systems or applications on Information Systems.

Passwords in readable form (e.g., written on paper) must be kept in a safe location and not stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.

Information systems and workstations must not display or print passwords as they are entered.

User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use. However, use of password retaining programs is allowed provided that the retaining program requires authentication and stores passwords in an encrypted manner.

Passwords must not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.

Passwords must be changed as follows:

At least every 90 days,

Immediately if discovered to be compromised or one suspects a password has been compromised,

Immediately if discovered to be in non-compliance with this standard, and on direction from management.

Do not reuse a password you have used any of the last 3 times you have changed your password, or more recently than 2 years from when you last used the password.

Access to password files or password databases must be restricted to only those who are authorized to manage the information system.

If a determination is made that a password has been compromised or is not in compliance with this standard, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.

Passwords for servers, mainframes, telecommunications devices (such as routers and switches), and devices used for information system security functions (such as firewalls,

intrusion detection, and audit logging) must be encrypted when stored electronically.

POLICY 19-09-788

ATTACHMENT D

Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area Network or the Internet.

Administrative level or system level passwords must be changed every thirty days

- b. **Sign-on Attempts and Device Lock-out Times**: A limit of 3 sign-on attempts and 600 seconds lock-out time will be allowed. Exception should be documented in the system security plan.
- c. **Electronic Signature Codes**: Electronic signature codes shall be treated as sensitive information requiring the same level of protection as individual access and verify codes.
- d. **Multiple Sign-on Restriction**: Requests for multiple sign-on are handled on a case by case basis and should include justification and concurrence by designated ISO with the exception of users that require multiple sign-on to use the GUI and other software packages simultaneously. All exceptions must be documented in the system security plan.
- e. **Timed Read**: The maximum time allowed shall be set to 300 seconds for users to prevent unauthorized access to unattended workstations with the exception of some clinical staff. Providers may receive timed read up to 900seconds for ease of use in clinical settings based on Clinical Application Coordinator (CAC) recommendations. Requests for increased timed read should be handled on a case-by-case basis, require justification, approved by the Facility CIO and should be submitted to the designated ISO for concurrence.
- f. **Screen savers**: Password protected screen savers are enabled for use as appropriate. The password protected screen savers are configured to activate after 15 minutes or less of inactivity. Only VA-approved screen savers will be used.
- g. **Session Lock**: Information systems prevent further access to systems by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system.
- h. **Programmer Mode Logs**: For users that have been granted the Programmer Mode option and the associated security keys, a programmer access code (PAC) shall be assigned for additional security. The Kernel will prompt for the PAC just before allowing the user to enter programmer mode. Programmer mode access will be approved by the Facility CIO and audited by the ISO.
- i. **File Access Security**: IT is responsible for granting file access. The supervisor and/or application coordinator will determine the needs of each user and the appropriate degree of access authority to be assigned. This must be reviewed on a yearly basis by the

approving official to ensure access is still necessary in the performance of the employee's duties.

POLICY 19-09-788

ATTACHMENT D

j. **Access scripts with embedded passwords are prohibited.**

Vendor supplied passwords are replaced immediately.

The Facility CIO and the ISO must approve specific user actions that can be performed on the information systems without appropriate identification and authentication (i.e., service accounts, site-to-site VPN accounts, training accounts in test system).

When possible, the information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.

As appropriate and indicated, the information system identifies and authenticates specific devices before establishing a connection (i.e., site-to-site VPNs, wireless)

As appropriate, the information system employs authentication methods that meet the requirements of FIPS 140-2

k. **General Windows System Security:**

Window 95, 98 and NT PC's will not be used as workstations on LAN due to lack of security. Special use configurations are exempt from this; i.e., visual impairment devices and medical devices.

The VHA04 and each local resource domain must be configured to audit.

Locked down or GENERIC ACCOUNTS are NOT allowed.

Keep systems up-to-date: Maintain information systems, such as servers, workstations, routers, etc., with up-to-date service packs and patches as they are released.

Router or other telecom devices: Assign passwords and SNMP (Simple Network Management Protocol) community strings that cannot be easily guessed and that are not the defaults. Use access lists to prevent unauthorized connections to the vty port and SNMP server.

Null NT/Active Directory sessions are prohibited.

All Active Directory accounts must utilize strong password authentication and exist only in VHA Primary LOGON Domains. VA's approved Active Directory architecture requires that all user accounts must conform to the national naming

conventions and also reside in approved VA primary domains (VHA04) as outlined in “Windows NT Enterprise Security Policy Implementation

POLICY 19-09-788

ATTACHMENT D

Help Desk Personnel must be provided clear procedure for validating a user identity before remotely clearing a password. These procedure should be document and available for review by outside auditors.

Access scripts with embedded passwords are prohibited.

Vendor supplied passwords are replaced immediately.

**Active Directory Administration Roles – Network 4 Domain (ADMINISTRATOR AND USER ACCOUNTS) and the Resource Domains:**

1. Membership in the VHA04 Administrators and VHA04 Domain Administrator group will be limited and controlled by the Network 4 WAN Managers. Exception: Service Accounts. Membership in Medical Organizational Unit (OU) will be made as deemed appropriate by the Medical Center. This will allow The Facility to create a balance between convenience and security, and provide a method of logically managing those user accounts most critical to the management of the Facility.
2. Domain and OU Administrators are required to change their Administrative account passwords every 30 days, rather than the usual 90 days for Domain Users. This will allow the Facility to remain within the requirements set forth by the Office of Cyber and Information Service (OCS).
3. Domain and OU Administrators utilizing any remote control tools such as SMS, Dameware, PCAnywhere, etc., must have the ability to audit actions taken on any remote systems and have all current patches installed. Domain and OU Administrators are prohibited from accessing another sites servers or workstation without prior approval of the remote site’s Information Management Service staff.

Prohibited Times for Sign-On: Time periods can be specified during which sign-on can be barred by device or by user.

**Vista Verify Codes and Active Directory Passwords:**

1. Prior to initial account distribution, positive physical identification of individuals receiving accounts shall be conducted. Positive physical identification can be done by anyone the system administrator can trust to perform such a task. For example, if an employee needs access to a system located off-site, the employee’s supervisor could make positive physical identification of the employee, and request access via electronic mail. During the first instance of access with a new account, the initial

password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.

POLICY 19-09-788

ATTACHMENT D

2. To ensure accountability, all user accounts must be individualized. The VistA verify code and Active Directory password for all user accounts must be changed every 90 days. To ensure that users change their verify codes at periodic intervals, Information Management Service shall set the Lifetime of Verify Codes and Active Directory passwords parameter to 90 days. Accounts that have been inactive for 90 days shall be disabled.
3. Embedded scripts that contain VistA access and verify code or Active Directory username and password are prohibited.
4. Controls shall be implemented to require strong passwords, per "Windows NT Enterprise Security Policy" approved by the VA CIO Council on January 21, 2000.
5. The Active Director and VistA strong password/verify code implementation consists of the following components:

The password must be at least 8 characters long, and can be no longer than 20 characters.

Active Directory and VistA system recognizes four classes of characters in passwords:

- Upper case letters (A - Z)
- Lower case letters (a - z)
- Numbers (0 - 9)
- Certain special characters. You may use only the following special characters:

~ (tilde)	` (accent mark)
! (exclamation mark)	@ (at sign)
# (pound sign)	\$ (dollar sign)
% (percent sign)	^ (carat)
& (ampersand)	( (open parenthesis)
) (close parenthesis)	{ (open brace)
} (close brace)	' (apostrophe)
. (period)	(space)

6. The Active Directory and VistA strong password/verify code must contain at least one character each from three of the four classes above. For example, use at least one letter, at least one number and at least one special character.

7. Active Directory passwords may not be your Active Directory account name, and they may not contain a segment of the Active Directory account name. VistA verify codes may not be the same as your VistA access code.

8. These policies are only applied to human user accounts. Service account passwords will be exempt from these restrictions. These are enforced by the Domain Account Policy POLICY 19-09-788 ATTACHMENT D

and, in the case of service accounts, are exempted from the Domain Account Policy restrictions in each service account's account properties. To meet VHA Security Requirements, the account policy that will be set in place will require:

Password length will be at least 8 characters.

ii. Passwords will expire every 90 days.

iii. Password Uniqueness or History = three (3) previous passwords will be remembered and not be allowed to be used.

iv. Account lockout after three (3) unsuccessful logon attempts.

v. After 10 minutes, your account will be unlocked and you will be able to log on again. (An administrator could also manually unlock an account before the 10 minutes expires).

#### **I. Audit Logs:**

Information Management Service staff, or designee, shall create, maintain and protect a security audit trail of user and administrator actions so that security relevant events can be traced to a specific user for accountability. Logs should be maintained at a minimum of six months and reviewed by the system manager, or designee, daily. The Facility ISO will audit this process to insure the reviewed events are corrected.

1. Windows Server Events Recorded: At a minimum a record should be written to the security audit trail for at least the following events:

i. Logon and logoff, both successful and failed events.

ii. Use of user rights, failed events only. Attempts to access objects (e.g., resources) or perform functions that are denied by lack of privileges or rights

iii. Security policy changes, both successful and failed events.

iv. User and group management, both successful and failed events.

- v. Restart, shutdown, and system, both successful and failed events.
- vi. Process tracking, failed events only.

2. Windows 2000/2003 Event Recorded. For each recorded event, the audit record shall identify, at a minimum:

POLICY 19-09-788

ATTACHMENT D

- i. Audit account logon events, both successful and failed events. Tracks user logon events on other computers in which the local computer was used to authenticate the account.
- ii. Audit account management, both successful and failed events. Tracks changes to the security account database (when accounts are created, changed, or deleted).
- iii. Audit directory service access, failed events only events. Audits users' access to active directory objects that have their System Access Control List (SACL) defined. This option is similar to audit object access except that it only applies to active directory objects and not files and registry objects. Since this option only applies to active directory, it has no meaning on workstations and member servers.
- iv. Audit logon events, both successful and failed events. Tracks users who have logged on or off, or made a Network connection. Also records the type of logon requested (interactive, Network, or service). This option differs from audit account logon events in that it records where the logon occurred versus where the logged-on account lives. Track failures to record possible unauthorized attempts to break into the system.
- v. Audit object access, failed events only. Tracks unsuccessful attempts to access objects (directories, files, and printers). Individual object auditing is not automatic and must be enabled in the object's properties.
- vi. Audit policy change, both successful and failed events. Tracks changes in security policy, such as assignment of privileges or changes in the audit policy.
- vii. Audit privilege use, failed events only. Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to administrators or other power users.
- viii. Audit system events, both successful and failed events. Tracks events that affect the entire system or the audit log. Records events such as restart or shutdown.

3. Windows Event Data: For each recorded event, the audit record shall identify, at a minimum:

- i. Data and time of the event

POLICY 19-09-788

ATTACHMENT D

- ii. User ID and associated point of physical access (e.g., node, port, Network address, or communication device)

- iii. Type of event

- iv. Names of resources accessed

- v. Success or failure of the event

4. VistA Audits: At a minimum, the following security audits for at least the following events:

- i. Sensitive record access on a daily basis

- ii. Programmer access on a monthly basis

- iii. Timed reads for Kernel and CPRS GUI on a monthly basis

- iv. File security access codes # and @ on a monthly basis

- v. Multiple sign-on review on a annual basis

- vi. Programmer Access Code (PAC) on a monthly basis

- vii. Menu option review on a quarterly basis

- viii. Security keys on a yearly basis

- ix. File security access for all users on a yearly basis

5. Passwords: Do not record passwords in the security audit trail

6. Reports: Generate audit trail reports regularly for review, or as immediately needed (e.g., when a system alarm detects a security problem)

## **2.0 Logical Access Controls (HIPAA 164.308a4iiB, 164.308a4iiC; FISMA 15.1, 16.1, 6.2.4, NIST 800-53 AC)**

### **Policy:**

Logical access controls are employed to permit only authorized access to VA computer systems and restrict users to authorized transactions, functions, and data. These automated controls ensure that only authorized individuals gain access to information system resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable for their actions. These controls support the separation of duties principle. Every user account is reviewed by management and



security staff annually with subsequent follow-up reviews every 90 days to ensure appropriate separation of duties and to ensure that the most restrictive set of rights/privileges or access needed by users is in place. Refer to Section 5.0 Audits and Reviews for Access Control Audits conducted.

**Procedure:**

POLICY 19-09-788

ATTACHMENT D

Access Permissions:

1. Facility CIO will maintain a current list of approved and authorized users and their access.
2. The Facility CIO or designee will process all requests for access in accordance with the facility's access policy.
3. System users will be prompted by the system to enter a new verify code and password every 90 days.
4. Accounts are automatically disabled if inactive for 90 days.
5. Application menus shall be created to permit the user to perform all duties required of his/her position and permit access to data for which the user has a need to know. The supervisor and application coordinator (ADPAC) responsible for the user will determine the appropriate menus. Responsibility and authorization for the creation or modification of application menus will be under the control of the Facility CIO or designee.
6. To ensure accountability, use of individual access codes and passwords are mandatory for all VA information systems. Only the individual to whom the codes were assigned will use their assigned codes. Guest accounts are not allowed on VA information systems, as this type of account exposes information systems to risk by allowing access through the use of a generic logon ID that requires no password or uses a widely known password. The use of shared and generic accounts on VA information systems is prohibited. In the event of lost or compromised password, the individual will notify the ISO or Facility CIO or designee, who will take appropriate measures.
7. Taping codes to equipment or furniture in work areas to avoid "memorizing" them is strictly prohibited. All codes allowing access to information systems are considered confidential information and must be treated as such.
8. Access to system security files, system management/configuration files, and creation of shared drives or other protected files is limited to IT staff that requires this access in order to perform their duties. Users with programmer access, system manager or Network administrator capabilities, which allow unrestricted access, shall not misuse access capabilities to view or modify anyone else's files and/or mail messages.

9. Staff who administer access control functions do not administer audit functions.

10. The Facility CIO or designee shall generate security codes for newly authorized facility users and when appropriate, existing authorized users and provides the codes in a secure manner to the user or responsible ADPAC. If an existing user has difficulty  
POLICY 19-09-788 ATTACHMENT D

accessing the system, IT will reset and allow the user to issue their own verify code or password after the user has been positively identified. Identification is required at the time a user receives password information.

11. The ISO will review all requests for system access by non-facility users. The request shall state the individual's name, SSN, telephone number, facility, and purpose for access, and shall have the concurrence of a higher level official within the requestor's facility or organization. Distribution of security codes for authorized non-facility users will be handled in the same manner as with local users.

12. Requests for access to remote systems must be approved by the user's supervisor and submitted to the ISO for processing.

13. In the event of an emergency, emergency access to sensitive information will be granted in accordance with contingency procedures. These accounts will be terminated immediately upon conclusion of the emergency situation.

14. In the event that temporary access is required (i.e. OIG/JCAHO) access will be provided and an automatic termination date established to ensure the account is terminated appropriately.

15. System managers and others with special system level access privileges are expressly prohibited from reviewing or accessing individual accounts or personal computers unless specifically authorized in writing or email by appropriate senior management officials and the ISO.

16. In the event of non-routine circumstances in which the employee possesses VA information and is not available, management officials may review an account or personal computer as part of their supervisory responsibilities. The following procedures have been established for obtaining such access:

Submit a request for access to a user's account or personal computer to the ISO and include, at a minimum, the following information: first and last name of user; username (account name); justification for access; location of files; location to save the files to (i.e. supervisor's drive or CD); duration of review.

Upon approval from the designated supervisor/manager, the ISO will coordinate requested access with the IT Chief/CIO. The ISO will not be the recipient of user's individual files from a facility storage device.

Audit logging for all activities related to this emergency access request is required and must be protected and saved.

POLICY 19-09-788

ATTACHMENT D

Emergency access must specify the person authorized to access the account. Under no circumstance will the unavailable individual's logon ID or password be used or compromised during emergency access.

The system administrator will rewrite the access rules to give the manager or designee access to the information (files).

Upon completion of the emergency access, all access to the information will be returned to the original state.

It is the responsibility of the user's supervisor/manager or designee to notify the unavailable individual of the emergency access as soon as he or she becomes available.

**b. Distribution of Access/Verify Codes and Active Directory Passwords for Network 4 Users and Non-Network 4 Users:**

1. **Network 4 Users:** The system manager, or designee, at each site shall generate security codes for newly authorized users and when appropriate, existing authorized users and provide the codes in a secure manner to the user or responsible ADPAC.
2. **Non-Network 4 Users:** Requests for system access by non-Network 4 users shall be requested in writing to the ISO at their respective site. The request shall state the individual's name, SSN, telephone number, facility, and purpose for access, and shall have the concurrence of a higher-level official within the requestor's facility. Distribution of security codes for authorized non-Network 4 users will be handled in the same manner as with local users.
3. **Security Forms:** Employees/non-employees are required to sign an established computer "Rules of Behavior", formerly known as VistA Access Agreements, at their duty station before access to information systems is allowed. Attachment A is the minimum "Rules of Behavior" for all Network 4 facilities.

**c. Access to Network 4 Information Systems:**

Individuals requiring Universal Access to ALL ten Network 4 VistA systems, Information Resource Center (VISN) SQL Server, or the Care Management Information Systems (CMIS) are responsible for completion of the Request for Network 4 Access form (Attachment D). All individuals who use or gain access to VA information systems or sensitive information must adhere to VA, VHA and Network policies, including patient confidentiality, access to sensitive data (including Electronic Protected Health Information) and appropriate use of electronic mail.

POLICY 19-09-788

ATTACHMENT D

**Each Medical Center Facility CIO or designee will be responsible for:**

Concurring and/or making alternate access recommendations on user requests, issuing and deactivating VistA and user access in a timely and accurate manner, and terminating VistA and Active Directory access in accordance with local medical center policy.

Creating and maintaining any Active Directory accounts from the applicant.

Terminating/disabling all non-VA employee(s) accounts at the termination date provided by the Contracting Officer and/or the Contracting Officer Technical Representative (COTR).

**The Contracting Officer is responsible for**

Ensuring that any applicable Background Investigations (following A&MM Information Letter 90-01-6) and Contractual Business Associate Agreement are in place.

The Contracting Officer and/or Contracting Officer Technical Representative (COTR) will provide a termination date for all non-VA employee(s) requests.

The Network 4 Chief Information Officer will be responsible for approving/disapproving Network 4 computer systems access requests for users. Chief Information Officer will forward approved access forms to VISN staff who will process requests based on priority; urgent requests processed within 24 hours; routine requests processed within 3 working days; low priority requests processed within 5 working days.

**Network 4 Universal VistA Access:**

Complete a Request for Network 4 Access Form (Attachment D). This form is to be completed and signed by the individual requesting access. Concurrences must be obtained from local Medical Center Service Chief/Service Line Manager/ Patient Care Center and/or Physician Leader, and Medical Center ISO.

Clinical staff will be assigned a generic menu, i.e., GMTS.

Requests for other than the approved clinical menu will be handled on a case-by-case basis. The requestor must specify the exact menu option requested and for multiple menu requests a menu diagram is required, why access is needed to certain files, etc., and obtain concurrence by the local Medical Center CEO and Medical Center ISO. A justification will also need to be included with the Request for Network 4 Access form, e.g. approved at 6/99 ELC. It should be noted that menus of this type could be

POLICY 19-09-788

ATTACHMENT D

more than read only as the Network 4 shifts its paradigm and reflects Network 4-wide initiatives.

The completed form is then faxed to the Network 4 Chief Information Officer (CIO) at 570-821-7235 for approval/disapproval and signature. The original request for access form is to remain at the local facility. Incomplete forms will be returned to the local facility.

Approved requests are then forwarded to the Network 4 ISO who will assign a standardized access code. On a weekly basis or as needed, the VISN ISO will transmit the assigned access codes and electronic copies of the approved Request for Network 4 Access forms via MS Exchange to the ISO at the local Medical Center who will handle in accordance with local policies and procedures.

Upon receipt of access codes, the Medical Center will have one week to issue/change/deactivate the requested user access.

Local OI&T Field Office will be responsible to setup individual communication methods at each site once user VistA access is granted by other VAMC's.

## 2. SQL Server Access:

In order to obtain access to the VISN Structured Query Language (SQL) Server, a Request for "Network 4 Access form" is to be completed and signed by the requesting individual. Concurrences must be obtained from the local Service Chief/Service Line Manager, and Medical Center ISO.

The completed form is then faxed to the Chief Information Officer (CIO) at 570-821-7268 for approval/disapproval and signature. The original request for access form is to remain at the local facility. Incomplete forms will be returned to the local facility.

VISN staff will be responsible for assigning access codes to users of the VISN SQL Server and notifying users when access is granted via an MS Exchange message.

## 3. Access to the CMIS:

Individuals requiring access through the Care Management Information System (CMIS) should complete and sign the Request for "Network 4 Access form". Concurrences must be obtained from the local Medical Center Director, and Medical Center ISO.

The completed form is then faxed to the Network 4 Chief Information Officer (CIO) at 570-821-7235 for approval/disapproval and signature. The original request for access form is to remain at the local facility. Incomplete forms will be returned to the local facility.

POLICY 19-09-788

ATTACHMENT D

VISN staff will be responsible for granting user access to the CMIS and notifying users when access is granted via an MS Exchange message. Account and password information will be transmitted to the Medical Center ISO.

c. Transfers/Termination of Employees:

When a user's status changes, the user's supervisor and assigned Application Coordinator will review the user's current authorizations, determine the need for continuing access/menu options, and forward to the ISO for necessary action. Appropriate action must be taken by the supervisor, Application Coordinator, ISO, and system manager to ensure the following:

1. Employee no longer has possession of unneeded sensitive data media.
2. Employee has returned all keys and access devices.
3. Employee security codes, electronic signatures, menu options, and security keys for both local and remote systems have been reviewed for either alteration or termination.
4. System managers of host systems providing access have been notified in a timely manner of user status change.
5. Supervisor debriefs the employee, discussing the regulations on safeguarding sensitive data used on the job to ensure nondisclosure to any unauthorized persons or agencies.
6. Office of Inspector General (OIG) Security Officer is notified if an employee leaves a position requiring a sensitivity level designation.
7. If an employee is a remote user and has been terminated, all ISOs in the Network 4 will be notified via the ISO Distribution List in Exchange/Outlook "VHA Network 4 04 IT ISO". Action will be taken to ensure that all access privileges are rescinded.

8. If an employee is a Public Key Infrastructure (PKI) user, all ISOs in the Network 4 will be notified via the ISO Distribution List in Exchange-Outlook "VHA Network 4 04 IT ISO". Action will be taken to ensure that their PKI certificate is revoked.

**e. Non-Employee Access:**

In contracts for hardware, software, and computer-related services, the Facility must ensure that appropriate security requirements and specifications are included in  
POLICY 19-09-788 ATTACHMENT D

statements of work, and security requirements and specifications are implemented properly before the system goes into operation. Patients are not permitted to utilize the VA Network for access to the Internet.

**Contractor Responsibilities**

Maintenance contractors and their employees shall be granted limited and controlled access to computer equipment and systems consistent with established security requirements.

All computer system contractors shall be required to meet the minimal security requirements defined in Section 1 - Personnel Security.

Contracts should stipulate that the contractor is responsible for the cost of background investigations, if required.

All default passwords on new or existing equipment must be changed before equipment installation to "strong" password format.

**2. Procurement Official Responsibilities**

Security requirements and specifications for hardware and software maintenance personnel contracted from commercial sources shall be defined and approved prior to the signing of contractual agreements.

Procurement officials shall ensure negotiated contracts pertaining to information management services include a separate section dealing with information security issues specifying the level of trust required and contractor responsibility in complying with established requirements.

Procurement officials shall ensure that all solicitations and purchase agreements pertaining to information management hardware and software are reviewed for security implications. Such officials are responsible for the inclusion of a separate section in the contract dealing with information security issues, where appropriate.

The Facility ISO shall advise the respective procurement officials if security specifications are adequate or need strengthening.

### **3. Other Contracts**

All non-VA users having access to VA information resources through a negotiated contract shall meet the minimum-security levels defined by the contract, prior to the effective date of the agreement. Such users will read and sign the “Rules of Behavior”,

POLICY 19-09-788

ATTACHMENT D

formerly known as VistA Access Agreements prior to receiving access to the Facility information systems.

Contract personnel security requirements are included in all contracts according to the Office of Acquisition and Material Management Information, Information Letter (IL 90-01-6).

The Contracting Officer Technical Representative (COTR) will work with the Information Manager, or designee, and ISO to determine the position sensitivity designation utilizing VHA Handbook 0710 “Personnel and National Information Security”. The Information Manager, or designee, shall ensure that all contracts pertaining to computer hardware and software are reviewed for security implications.

#### **Distribution of Public Key Infrastructure (PKI) Certificates:**

To address VHA Directive 6210 that requires the protection of sensitive information transferred between external “untrusted” Networks and internal, “trusted” Networks, all sensitive information must encrypted with Public Key Infrastructure (PKI) whenever possible.

1. The ISO, or designee, will process all applicable requests for Public Key Infrastructure (PKI) certificates in written or electronic request to the NISO. All VA employee requests must have the requestor’s name, station number, and E-mail address. All contractor/third-party requests must have the requestor name, company name, street address, city, state, zip code, phone number and E-mail address.
2. The ISO will assist PKI users in the proper usage and education of PKI technology.
3. The ISO shall request the NISO to revoke PKI certificates as appropriate.
4. All new PKI users will publish their digital certificate to the global address list (GAL). This will allow facility employees with PKI certificates to send and/or receiving encrypted messages with other VA Employees.



**d. Rights Management Services (RMS).**

Facility CIO's must ensure that Rights Management Services are available and operational within Network 4.

Microsoft Windows Rights Management Services enables users to protect electronic documents and email messages by designating not only who is allowed to access the  
POLICY 19-09-788 ATTACHMENT D

content of the documents or emails but also by controlling what may be done with them after they have been opened. These controls are sometimes called usage rights or usage policies.

Example: A VA employee will be able to send an "RMS protected" email message to other VA employees and control whether or not the email can be forwarded to anyone else, copied or printed.

RMS is not a substitute for PKI (Public Key Infrastructure). PKI should be used to digitally sign a message.

RMS prevents forward and printing of messages.

PKI only protects the message while it is being transmitted. RMS manages what's done with the message by the recipient

When messages containing sensitive information are sent outside of the VA network PKI must be used no exceptions.

**e. Read Only Access:**

Accredited Veteran Service Officers (VSOs) and people holding valid Power of Attorney (POA) may be given read only access to the electronic record. Access may be granted only when consent is received from the patient or when a valid POA form is presented. Access will not be given to the entire patient database, only to those patients the VSO or POA has legal authority to view. As with all other people granted access to the electronic record, the VSO or POA must complete a Cyber Security Awareness Course and sign the National Rules of Behavior statement prior to receiving access. Remote access for VSOs or POAs will not be granted.

**f. Screen Savers:**

Password protected screen savers are enabled for use as appropriate at this facility. The password protected screen savers are configured to activate after fifteen minutes or less of inactivity. Only VA-approved screen savers will be used.

### **Encryption:**

Confidential or patient-sensitive data may not be transmitted via Internet or VA's internal Network (Intranet) without proper security mechanisms that meet NIST's FIPs 140-2 criteria. The VA has chosen PKI as the current solution for transmission of sensitive information over the VA Intranet. ISOs are responsible for ensuring that users who have POLICY 19-09-788 ATTACHMENT D

a need for VA PKI receive appropriate training and support. ISOs coordinate requests for VA PKI certificates with the Local Registration Authority (LRA). ISOs may be required to perform Identity Proofing Procedures to securely and confidentially distribute VA PKI enrollment information to participants.

### **Internet Gateway:**

The Facility will use the national gateways to access the Internet. The national gateways are configured to restrict information flow based on an approved rule set. Users will use the Internet in a secure manner. All users must adhere to the national and local Internet access and usage policy when accessing the Internet and understand that Internet activity is monitored. NO PATIENTS are allowed use of the VA network for Internet access.

### **Remote Access:**

The site documents, monitors, and controls remote access to the information systems including remote access for privileged functions.

Remote Access is allowed and controlled through the National One VA VPN. The National One VA VPN controls all remote accesses through a managed access control point. All requests for One VA VPN accounts must obtain the proper concurrences as required by Attachment A of the Medical Center policy **19ISO-09-406-USE OF REMOTE ACCESS SERVICES ONE VA VPN.**

In recognition of its responsibility to secure and safeguard information from misuse or improper disclosure, all remote access service computer users must provide proper justification of the need for access, and sign the National Rules of Behavior prior to remote access being granted. Approved remote access users can access VA systems from their residence or while they are on travel status using approved government furnished equipment (GFE). If non-VA owned equipment must be used in certain circumstances, a waiver must be in place. All of the security controls required for GFE must be utilized in approved non-VA owned equipment and must be funded by the owner of the equipment.

Approved remote access users are governed under the same local policies, federal laws and regulations that apply to all local users of VA computer systems and the security and privacy of the information contained therein.

Responsibility for access to, or training on, systems not covered by this policy lies solely with the individual or service/section requiring this access. Remote access to VA computer systems does not constitute approval for overtime pay or compensatory time.

OI&T staff is responsible for ensuring that the requestor receives instructions on how to setup the PC or laptop for the required access and for providing any needed assistance. If

POLICY 19-09-788

ATTACHMENT D

the remote access user needs assistance with configuring this access or to determine hardware compatibility, they should follow their local Helpdesk procedures.

If a remote access account request is disapproved, the requester and his/her service chief will be notified and an explanation for disapproval will be provided. If the requester's requirement for remote access changes, the request may be resubmitted.

New users (those who do not have a current VA Network account) who request remote access must complete HIPAA Privacy and Information Security Awareness training, and complete the authorization for IT access before any access can be granted.

**Remote (Off-site) Users:** Requests for access by remote users will be submitted in writing to the ISO including the user's name, service, phone number, mail code, social security number and purpose for access, and will have the concurrence of a higher level official within the user's facility. The appropriate documentation will be coordinated with the remote facility ISO and forwarded to the ISO. Codes for authorized remote users will be delivered either electronically using PKI or in a sealed envelope to the remote facility's ISO. The user's name and the statement, "TO BE OPENED BY ADDRESSEE ONLY" will be annotated on the outside of the envelope. Users should contact their ISO if the envelope is not sealed when delivered.

**Contractors/Non-VA Staff:** Requests for access by non-VA staff will be submitted in writing to the ISO and the CO or COTR to include the user's name, service, phone number, mail code, social security number and purpose for access. All non-VA staff is required to follow the same policy and procedures and will have the concurrence of a higher level official within the facility they are requested access to. The appropriate documentation will be coordinated with the contractor/non-VA staff by the CO / COTR and ISO. Codes for authorized remote users will be delivered either electronically by PKI or in a sealed envelope to the ISO or to the CO or COTR for distribution to the contractor or non-VA staff.

**Transferring, Retiring or Terminating:** Users who have a One-VA VPN account whether transferring/terminating/retiring need to notify the ISO. The ISO will

periodically audit all VPN accounts to ensure they are still needed as specified in VA Handbook 6500.

ISOs are responsible for auditing remote access authorizations and ensuring remote access users know how to use the remote access connection securely. ISOs ensure that remote access privileges are terminated promptly when they are no longer required as specified in VA Handbook 6500.

### **External Business Partner Connections**

POLICY 19-09-788

ATTACHMENT D

Data communications pathways from the VA Network to non-VA business partners that cannot pass through the One-VA Internet gateways must be fully documented, must have Facility CIO and ISO approvals and be approved by OI&T.

Modems may not be installed on workstations and systems connected to the VA Network. If a dial-in connection is considered essential to a program mission, the facility must complete and have on file a waiver request form and obtain approval from OI&T. If approved, security controls and procedures will be documented in the security documentation for the affected system and maintained for future information security audits and inspections. Stand-alone systems not connected to the VA Network must develop and document a procedure for remote diagnostics and maintenance of equipment that is tightly controlled. Event logging functions are to be provided to enable the review of suspicious activity. Only remote control software configured and approved by OI&T and the Facility CIO may be used to control VA systems via the LAN, WAN, or remote access.

### **Wireless Access Restrictions (NIST SP 800-53 AC-18)**

#### **Wireless devices:**

All wireless technology equipment transmitting sensitive information must utilize a VA approved encryption methodology (AirFortress for BCMA). To minimize the risk, the following measures shall be implemented.

FIPS 140-2 Encryption of information transmitted to and from a wireless device is required or an appropriate waiver has been approved by the CIO.

Wireless devices must meet and be kept up-to-date on the latest anti-viral and software/security patch remediation, as applicable.

Authentication is required to protect wireless access to the information system.

### **Mobile Code**

The site has (i) established usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Facility CIO authorizes the use of mobile code.

### **Voice Over Internet Protocol (Not implemented at this time)**

The site has (i) established usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

### **Facsimile (Fax) Machines:**

Care should be taken to assure confidentiality when faxing sensitive or confidential information. Following are the precautions that should be taken to protect the security of fax transmissions:

The following statement must be included on all fax cover sheets: "This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

(The HIPAA Security Rule does not apply to faxing because the information is not in electronic format prior to sending. The HIPAA Privacy Rule requirements do, however, apply. In the event that a fax is sent via automated systems, or fax back from a computer, then the HIPAA Security Rule does apply because the information was already in electronic format before it was transmitted.)

Staff is instructed to double check the recipient's fax number before transmittal and to confirm delivery by telephone or review of the appropriate confirmation of fax transmittal.

Fax machines are placed in areas that require security keys, badges, or similar mechanisms in order to gain access.

Staff periodically reminds regular fax recipients to provide notification in the event that their fax number changes.

Fax transmittal summaries and confirmation sheets are saved and reviewed periodically for unauthorized access or use.

Staff have pre-programmed and tested destination numbers in order to minimize the potential for human error.

### **PBX Voice/Data Telephone Systems:**

PBX security includes maintaining an audit trail to capture the date, time, user(s), and activities performed on the PBX system and implementing adequate investigations and audit methods to ensure appropriate and authorized access to the PBX system. To reduce exposure to security risks, the following actions should be taken:

- 1) Assign authorization codes randomly on a need-to-have basis.
- 2) Safeguard authorization codes and change them frequently.
- 3) Limit remote access trunks to domestic calling.
- 4) Implement the time-of-day PBX option.
- 5) Implement a system-wide barrier code.
- 6) Do not use or allow the use of trivial passwords such as "1111" or "2222".
- 7) Do not include programmable function keys or speed dialing keys in the password.
- 8) Monitor telephone bills regularly, looking for increased activity. If increased activity is suspected, contact the telephone vendor to request an audit of the PBX systems to determine if fraud has occurred. Use of the PBX system to monitor telephone calls must be authorized by the Facility Director.
- 9) All unused telephone jacks should be disabled as soon as possible to prevent unauthorized usage.
- 10) Third parties or third party systems that connect to this system must adhere to these procedures.

### **Electronic Mail (HIPAA 164.312e1):**

Electronic mail shall be used for authorized government purposes and shall contain only non-sensitive information unless the data is appropriately secured. Electronic mail users must exercise common sense, good judgment, and propriety in the use of this government resource. Electronic mail is not inherently confidential and users should have no expectation of privacy when using government mail systems. A technical or administrative problem sometimes causes a situation where a system manager or management official may need to review electronic mail messages. The ISO will provide concurrence for requests for removal of electronic mail messages when warranted.

Auto-forwarding of email messages to addresses outside the VA Network is strictly prohibited.

### **Medical Device Isolation Architecture:**

All medical devices that are currently or planned to be connected to the VA Network must follow the "Department of Veterans Affairs Medical Device Isolation Architecture Guide" dated April 30, 2004.

### 3.0 Log-on Warning Banners (HIPAA 164.310b)

**Policy:** Public Law 99-474 requires that any system that uses external communication mediums (e.g. dial-up, Internet, etc.) must have a warning banner that appears before the log-on sequence. If technically capable, the information systems within this [Operating Unit's Name] will display an approved, system use notification message before granting system access informing potential users : (1) that the user is accessing a U.S. Government information system; (2) that system usage may be monitored, recorded and subject to audit; (3) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (4) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices and remains on the screen until the user takes explicit actions to log on to the information system.

**Procedure:** The Facility CIO will coordinate with the system owners, system managers, and IT personnel to ensure that VA approved logon warning banners are deployed on all VA computer systems, including servers, workstations, routers, switches, and other devices that can accommodate the VA approved banner within their area of responsibility. The ISO will perform regular audits to ensure all capable equipment displays the warning banner.

### Logon Background Screens

**\*\* WARNING\*\*WARNING\*\*WARNING\*\***

"This U.S. Government computer system is for official use only. The files on this system include federal records that contain sensitive information. All activities on this system may be monitored to measure Network performance and resource utilization; to detect unauthorized access to or misuse of the system or individual files and utilities on the system, including personal use; and to protect the operational integrity of the system. Further use of this system constitutes your consent to such monitoring. Misuse of or unauthorized access to this system may result in criminal prosecution and disciplinary, adverse, or other appropriate action."

**\*\*WARNING\*\* WARNING\*\* WARNING\*\***

Displaying identifying information about the computer system or using "WELCOME TO . . ." is prohibited.

### 4.0 Penetration Testing and Vulnerability Scanning (HIPAA 164.308a1i)

**Policy:** Penetration testing and vulnerability scanning will be used by the VA NSOC to assess the strength of security controls of the systems within the Facility. Vulnerabilities discovered from scans and penetration testing will be reviewed and corrective actions taken by the system owners, system managers, and IT personnel. The site performs vulnerability scans regularly or when significant new vulnerabilities affecting the system are identified and reported.

**Procedure:** IT and the ISO should be trained in the use and maintenance of vulnerability scanning tools and techniques. The information obtained from the vulnerability scanning process is freely shared with appropriate

personnel throughout the facility to help eliminate similar vulnerabilities in other information systems. However, vulnerability scans are considered to be sensitive information and should be distributed, maintained and disposed of appropriately.

Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. Each facility will update the list of information system vulnerabilities as required or when significant new vulnerabilities are identified and reported. This process may be conducted independently or as a coordinated effort with the VA SOC.

System owners, system managers, and IT personnel will periodically review their systems to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, IIS).

## **5.0 Audits and Reviews (HIPAA 164.312b; FISMA 17.1.1, NIST SP 800-53 AC-2, AC-13, AU-3, AU-4, AU-5, AU-6, AU-11)**

**Policy:** Each site regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. Network 4 employs automated mechanisms, when applicable, to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Each site also periodically reviews changes to access authorizations. Each site undergoes periodic technical and non-technical IT security reviews, both internal and external. The results of all reviews/audits are securely maintained.

### **Procedure:**

#### **External Reviews:**

The following groups perform external security reviews that focus on both FISMA and HIPAA security requirements:

**Office of Inspector General** - CAP Reviews and security investigative reviews as mandated by the “Federal Information Security Management Act of 2002.”

**OI&T** - performs on-site security reviews

**JCAHO** (Joint Commission on Accreditation of Healthcare Organizations) - performs periodic reviews.

VA-NSOC conducts penetrations studies when requested.

Office of Compliance (OC)

The facility may request or fund additional security reviews as required.

#### **Internal Reviews:**



Activity involving access to and modification of sensitive or critical files is logged, monitored, and possible security violations investigated. At a minimum, the following internal reviews are conducted:

**System Auditing:** System audit logs must record sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Additional details such as type, location, and subject are also required for moderate and high risk systems. Audit logs will be maintained as follows:

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred.

Audit logs must be treated as restricted information and must be protected from unauthorized access, modification, or destruction; and reviewed periodically for action. Access to logs must be granted based upon need to know and least privilege.

Audit logs must be backed up and stored off-site.

The system administrator allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate IT staff and either overwrites the oldest audit records, shuts down the system, or stops generating audit records. A written risk based decision will be made for individual systems as to what happens when capacity is reached.

Audit logs must be retained for one year or as directed by the VA Records Officer.

Audit logs must be reviewed periodically for potential security incidents and security breaches. Audit logs may be reviewed to evaluate the damage caused by a security breach and also may support the recovery of data lost or modified. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).

**Log-in monitoring:** When a lockout occurs, the IT system manager will investigate to determine whether the action was that of an authorized user or an attempt to intrude. If it appears to be an intrusion attempt, the IT system manager will notify the ISO and the VA-NSOC.

Although they work in conjunction, there is a separation of duties between the ISO who reviews the audit trails and the system manager who administers the system.

**Sensitive Record Audit:** In accordance with VA policy, certain medical records are deemed sensitive and access to such records is monitored. The sensitive record access log will be monitored on a regular basis by the ISO and in accordance with ISO standard operating procedures. Supervisors/managers or designee in coordination with the ISO will exercise reasonable controls to ensure that employees cannot obtain access to other employee medical records except when they need to have access to the records in order to perform their official duties. If an employee obtains access to another employee's medical record without having the requisite need for access to the record to perform his or her duties, the employee who obtained access could be subject to disciplinary action and/or criminal penalties. Employees that need to review their own record or require copies

of their record must present a written request the Employee Health Nurse or Release of Information section to obtain this information. Veteran employees must contact their local Release of Information section to review or receive copies of their record.

**Incident-triggered Audits:** Investigation of an incident may necessitate a focus review audit. Facility CIO and ISO will collaborate in the audit.

**Data Access Controls/Security Keys:** The ISO reviews the access logs and security key allocations in Vista on a regular basis, at least quarterly, so that each individual's access is restricted to only those functions necessary to perform their duties. Using appropriate tools, such as NetIQ, account policies and restrictions are monitored in Windows 2000 Active Directory in order to determine how password and logon policies are enforced for the entire domain. The status of each user account can be checked in the User Manager. Appropriate security logs for Windows 2000 Active Directory must be enabled and reviewed routinely to ensure that security controls are in effect.

**Menu Reviews:** Employee menus (access) are reviewed at least quarterly to ensure that employees are restricted to the menus necessary to perform their duties. Menu adjustments will be made accordingly by the service and audited quarterly by the service and the ISO.

#### **1. User Reviews:**

[Vista]: Account status is reviewed by the supervisors/managers and the ISO on a quarterly basis to assure the need for account continuation. All accounts unused for more than 90 days are placed in disuser status and thereby made inoperable. Disuser accounts are terminated within one year unless the user's supervisor/manager certifies, in writing, the need for continuation of access. Disuser and terminated accounts are inactive. All user accounts of separated employees, contractors, volunteers, or any other user no longer requiring access will be terminated immediately.

**Network :** Account status is reviewed by IT and reported to the supervisors/managers and the ISO on a quarterly basis to assure the need for account continuation. All accounts unused for more than 90 days are placed in disabled status and thereby made inoperable. Disabled accounts are terminated within one year unless the user's supervisor/manager certifies, in writing, the need for continuation of access. All user accounts of separated employees, contractors, volunteers, or any other user no longer requiring access will be terminated immediately.

**FISMA:** Management, operational and technical security controls are reviewed each year by completing the annual FISMA Survey and regularly updating the FISMA/SMART database. New security questions/issues are added to this survey and database as required. This questionnaire helps to identify security deficiencies within the systems. The ISO will ensure the annual completion of the FISMA Survey and will oversee the addressing noted deficiencies via the POA&Ms (Plan of Action and Milestones).

**HIPAA:** The VHA HIPPA Program Management Office has provided the field a HIPAA Self-Assessment Tool that this facility utilizes to ensure HIPAA compliance.

Security Documentation Review: The ISO will conduct an annual review with the system owner, system manager, and IT personnel of security documentation for each system within the facility. Documentation will be updated as accordingly.

## **ACRONYMS**

A&MM - Acquisition and Materiel Management

AIS – Automated Information System(s)

ADP – Automated Data Processing

ADPAC - Automated Data Processing Application Coordinator

C&A - Certification and Accreditation

CA - Certification Agent

CMR - Consolidated Memorandum Receipt

COTR - Contracting Officer's Technical Representative

DAA - Designated Approving Authority

DOD - Department of Defense

EPHI - Electronic protected health information

Fax - Facsimile

FCIO – Facility Chief Information Officer

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Management Act

HIPAA - Health Insurance Portability and Accountability Act

IATO - Interim Authority to Operate

ID – Identification

IRB Institution Review Board

ISO – Information Security Officer

IT - Information Technology

JCAHO - Joint Commission on Accreditation of Healthcare Organizations

LANs - Local Area Network

MOU - Memorandum of Understanding

NIST – National Institute of Standards and Technology

OCS - Office of Cyber and Information Security

OCS – Office of Cyber Security

OIG - Office of Inspector General

OMB - Office of Management and Budget

PAC - Programmer access code

PDA - Personal Digital Assistant

PIA Privacy Impact Assessment

POA&M - plans of actions and milestones

R&D Research and Development

RFP - Request for Proposal

RID - Review and Inspection Division

SDLC - System development life cycle

SIA - System Interconnection Agreement

SMART – Security Management and Reporting Tool

SOW - Statement of work

SSN - Social Security Number

SSP - System security plan

TCP/IP - Transmission Control Protocol/Internet Protocol

POLICY 19-09-788

ATTACHMENT E

TEMPO - Training and Education Management Program

VA-NSOC - Veterans Administration Network and Security Operations Center

**VISTA** - Veterans Health Information Systems and Technology Architecture

WOC - Without Compensation